PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of	)	
	)	
Applicants: Bret A. Lowensohn et al.	)	
	)	**Examiner**
Serial No. 10/058,233	)	**Venkatanarayanan Perungavoor**
	)	
Filed: January 25, 2003	)	**Art Unit 2132**
	)	
Title: Portable Wireless Access for Computer-Based Systems	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

DECLARATION OF PRIOR INVENTION UNDER 37 C.F.R. §1.131

I, Bret A. Lowensohn, hereby declare that:

1. I am one of the co-inventors named in the above-identified application, and I am now the record owner by assignment of the entire right, title and interest in that application.

2. During the years 2000 and 2001 when the events recited below occurred, I was employed by Kaiser Foundation Hospitals (hereinafter "KFH"), a nonprofit, public-benefit corporation that owns and operates community hospitals in California, Oregon, and Hawaii; owns outpatient facilities in several states; provides or arranges hospital services; and sponsors charitable, educational, and research activities.

3. During my employment by KPH in the years 2000 and 2001, I served as Director, Advanced Technologies for Kaiser Foundation Health Plan / Hospitals, 393 E. Walnut, Pasadena, CA . During this period, I directed, and participated in the "Biometric Authentication and Roaming Badge Technology Project" (hereinafter the "BARB Project") conducted by KFH which resulted in the design, development, construction, testing and operation of badge-based authentications

system described in the above-identified patent application which I will hereinafter refer to as the "BARB Pilot System." I have direct personal knowledge of the facts set forth in this declaration.

4. The BARB Pilot System is described and claimed in the above-identified patent application. That system consisted of an administration subsystem (shown in the block diagram Fig. 5 of the application) that communicated with one or more "BARB Badges" (shown in the block diagram Fig. 2 of the application) by way of one or more "BARB Base" stations (shown in block diagram Fig. 3 of the application).

5. The BARB Pilot System described and claimed in the application was conceived in its entirety before January 26, 2001 as shown by Exhibits B, C and D which are all dated on or before that date. Exhibits B, C and D formed the basis for, and contain substantially the same technical disclosure as, the above-identified patent application as more fully detailed in paragraph 15, below.

7. Exhibit A is a true copy of the "CONTRACTING SERVICE AGREEMENT" entered into between KPH and a first contractor, Saflink Corporation, on September 22, 2000 (see "Date of Issue" on page 2 of the AGREEMENT). Pursuant to this agreement, Saflink developed the software for the administration subsystem for the BARB Pilot System in accordance with the requirements and functional specifications provided to Saflink by KFH. As provided in this AGREEMENT, Saflink Corporation was to complete and deliver the software for the administrative subsystem, along with system documentation, on or before January 31, 2001.

8. Exhibit B is a true copy of Version 1.2 of the "System Functional Specification, Biometric Authentication and Roaming Badge Technology Project" dated "26 January 2001" that describes the administrative subsystem software supplied by Saflink. The Function Specification, Exhibit B, was used as the source of the major portion of the disclosure found in the above-noted application and the correspondence between the two disclosures may be verified by comparing the drawing figures in the above-noted application with the corresponding drawing figures found in the functional specification as indicated in paragraph 15 below.

9. Exhibit C is a true copy of a contract proposal entitled "TagSense Wireless Identification and Data Interface" submitted to KFH by a second contractor, TagSense, Inc., on or about September 13, 2000 (see "Parts Availablity" in part VIII and part VII. Schedule). Pursuant to this proposal, TagSense developed and delivered three elements of the BARB Pilot

System consisting of BARB Badges, BARB Base stations, and a software SDK (System Development Kit) used by application programs (such as the administration subsystem developed by Saflink Corporation) to communicate with the base station and to access the BARB Badges via the base station. As stated in Exhibit C, TagSense agreed to deliver the badge and base station hardware, as well as the software for communicating with the badge and base stations, on or before November 4, 2000. The description of the badge and base station hardware and software functions contained in the above-noted application and discussed in connection with Figs. 2 and 3 of the application drawings is based upon and corresponds to the description found in Exhibit C.

10. Exhibit D. is a three page typed listing, also dated September 13, 2000, defines the interface specification for the API (Application Program Interface) that was to be provided by the TagSense SDK.

11. During the period which began at least as early as September, 2000 when detailed product specifications were provided to the two contractors, I and other members of the KPH team working on the BARB Project, including the seven named co-inventors named in the above-identified patent application, as well as the personnel assigned to this project by the contractors TagSense, Inc. and Saflink Corporation, were engaged in a substantial, continuous, diligent effort to reduce the BARB Pilot System to practice. As described in more detail in the following paragraphs 12-14, this continuous diligent effort resulted in an actual reduction to practice of the BARB Pilot System at least as early as May 9, 2000.

12. It is my belief that the BARB Badge, Base Station and the software SDK were reduced to practice and delivered to KPH by TagSense, Inc. pursuant to the proposal, Exhibit C, and that these components, as described in Exhibit C and as provided by TagSense were successfully operated and tested at KPH prior to the end of 2000.

13. It is my belief that the BARB management subsystem software was completed and delivered to KFH by Saflink, Inc. pursuant to the AGREEMENT, Exhibit A, on or before February 1, 2000 and that the management subsystem software described in Exhibit B as provided by Saflink was successfully operated and tested at KFH on or before March 1, 2000.

14. The BARB Pilot System as described in Exhibits B, C and D had been reduced to practice and was being tested by May 9, 2001. Exhibit E, a "Video Script" entitled "BARB Test

Announcement," describes a demonstration of the BARB Pilot system in actual operation that was presented to KFH hospital employees, the intended users of the system.

15. The disclosure contained in the above-identified patent application was based on and is a rewritten version of the disclosure found in Exhibits B, C and D as may be readily confirmed by a comparison of these disclosures. The correspondence between the numbered figures of the application drawings and the drawings found in the Functional Specification, Exhibit B, and in TagSense Proposal, Exhibit C, is set forth in the list below:

Application	**Source Document**
Fig. 2	Tagsense Proposal (Badge Hardware)
Fig. 3	TagSense Proposal (Base Station Hardware)
Fig. 4	Functional Specification Fig. 1
Fig. 5	Functional Specification Fig. 2
Fig. 6	Functional Specification Fig. 3
Fig. 7	Functional Specification Fig. 4
Fig.8	Functional Specification Fig. 5
Fig. 9	Functional Specification Fig. 6
Fig. 10	Functional Specification Fig. 7
Fig. 11	Functional Specification Fig. 8
Fig. 12	Functional Specification Fig. 24
Fig. 13	Functional Specification Fig. 9
Fig. 14A	Functional Specification Fig. 14
Fig. 14B	Functional Specification Fig. 25
Fig. 15A	Functional Specification Fig. 18
Fig. 15B	Functional Specification Fig. 26
Fig. 16	Functional Specification Fig. 20
Fig. 17	Functional Specification Fig. 21
Fig. 18	Functional Specification Fig. 22
Fig. 19	Functional Specification Fig. 23

16. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Dated: December 15, 2005 Signed by: Brent A. Lowensohn

Brent A. Lowensohn

KAISER PERMANENTE

Sample

CONTRACTING SERVICES AGREEMENT

SAFLINK CORPORATION

C.I.S. Security Enhancement Pilot ← = BARB

Date of Issue: SEPTEMBER 12, 2000

Revision: ____

SAFLINK Project Team

Walter G. Hamilton, V.P. Business Development
(425)881-6768 e-mail: whamilton@saflink.com

Cathy Tilton, Director of Special Projects
(703)708-9280 e-mail: cattilton@aol.com

Kaiser Project Team

Brent Lowensohn, Ph. D.
(626)405-5347 e-mail: brent.lowensohn@kp-research.org

Bill Woodmancy - Consultant Specialist Lead
(626)405-5371 e-mail: bill.woodmancy@kp-research.org

EXHIBIT A

Table of Contents

CONTRACTING AGREEMENT

THIS AGREEMENT is entered into on this ____ day of _____, **2000**, by and between **SAFLINK CORPORATION**, a Delaware corporation, with its principal office located at **18650 N.E. 67th Court, Suite #210, Redmond, Washington, 98052** (hereinafter collectively referred to as "**SAFLINK**"), and **KAISER FOUNDATION HOSPITALS**, a California nonprofit public benefit Corporation with an office located at **393 EAST WALNUT STREET; 6TH FLOOR, PASADENA, CALIFORNIA 91188** (hereinafter collectively referred to as "**KAISER**").

1. **DEFINITIONS**:

1.1 "**Statement of Work.**" A written document setting forth the Contracting Services (as defined in the Statement of Work) and Deliverables (as defined in the Statement of Work) (collectively, "Services") to be provided by SAFLINK to KAISER under this Agreement as mutually agreed upon by and between the parties, of which is substantially specified in the "Statement of Work" attached hereto, labeled **Exhibit "A"**, and incorporated herein by reference.

1.2 "**SAFLINK Methodology.**" Consists of pre-existing:

(i) know-how and methodology;

(ii) personal and professional programming techniques;

(iii) computer program algorithms; and

(iv) system design, architecture, logic, structure, sequence, and organization developed or known by SAFLINK prior to the commencement of the Services.

1.3 "**SAFLINK Modules.**" Pre-existing computer program modules proprietary to SAFLINK which SAFLINK may use to provide the Deliverables.

2. **SERVICES**:

2.1 **Services.** SAFLINK shall provide to KAISER the Services which constitute the Statement of Work in accordance with the terms and conditions hereof and the attached Statement of Work as referenced hereinabove.

2.2 **Change Orders.** Any change in the specified scope of Services and as set forth in the "Statement of Work" shall be mutually agreed upon by the parties in writing. The parties may utilize their standard Change Order Procedure to document these changes.

2.3 **Progress Reports.** SAFLINK shall provide KAISER with detailed reports from time to time regarding the progress of the Services as required under the Statement of Work, any anticipated problems (resolved or unresolved), and any indication of delay in fixed or tentative schedules.

3. **MUTUAL RESPONSIBILITIES OF PARTIES**:

3.1 **Party Contact(s).** Each party shall designate certain employees as principal points of contact for communication purposes regarding technical and business issues hereunder. Either party may change their respective technical and/or business contacts by written notice to the other.

3.2 **Cooperation.** The parties acknowledge and agree that certain data, information or assistance may be required from time to time in order for the parties to meet their obligations and exercise their rights hereunder, and upon written request by either party to provide same, shall furnish to the other, any and all pertinent and/or relevant documentation in their possession, pursuant to and in accordance with Section 7, hereinbelow.

4. **FEES AND EXPENSES:**

4.1 **Fees for Services.** Unless otherwise expressly specified in the applicable Statement of Work:

(i) The Services shall be provided on a "fixed-fee" basis, representing the entire project and encompassing any and all services and deliverables to be provided by SAFLINK to KAISER in accordance with the Statement of Work as referenced hereinabove.

4.2 **Invoicing and Payment.** SAFLINK shall invoice KAISER pursuant to and in accordance with the "Fixed-Fee and Payment Schedule", attached hereto, labeled Exhibit "B", and incorporated herein by reference.

5. **PERSONNEL:**

5.1 **Responsibility for SAFLINK Employees.** All personnel provided by SAFLINK to perform any Services under this Agreement shall be considered SAFLINK employees or agents, and SAFLINK shall be responsible for payment of fees or salaries (including the withholding or payment of all payroll or income taxes), worker's compensation, disability benefits and the like for such personnel.

5.2 **Insurance.** Contractor agrees to maintain insurance policies as follows:

* $1,000,000.00 **General Indemnity**
* $1,000,000.00 **Automobile Liability**
* $ 500,000.00 **Worker's Compensation**

Contractor agrees to keep the above policies in full force during term of this agreement. Contractor agrees to provide Kaiser with Certificates of Insurance as evidence that required coverage is in effect.

6. **INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:**

6.1 **Reservation and Grant of Rights.** Each party acknowledges that all patents, copyrights, trade secrets or other proprietary rights in or to the work product that SAFLINK may create for KAISER under this Agreement. (the "Deliverables") shall be owned by KAISER, and SAFLINK hereby agrees to assign such rights to KAISER, subject to SAFLINK's rights in any SAFLINK pre-existing works that may be incorporated into or embodied in any Deliverable; and SAFLINK hereby grants to KAISER a non-exclusive irrevocable license to use any SAFLINK pre-existing works to the extent incorporated into or embodied in any Deliverable, subject to mutually agreed license fees. Both parties agree that either party may use at any time and for any purpose all ideas, concepts, inventions or techniques that may be used, conceived or first reduced to practice in connection with the Deliverables. KAISER hereby grants to SAFLINK the non-exclusive, non-transferable, irrevocable, royalty-free and worldwide right to reproduce, display, distribute, modify, create derivative works based upon and otherwise market and maintain the Deliverables, directly or indirectly, to and for SAFLINK's customers; provided, however, that SAFLINK agrees not to directly distribute the Deliverables to any customer primarily in the health care industry for a period of 12 months after development of the Deliverables. During and after the term of this Agreement, SAFLINK and KAISER will execute the instruments

that may be appropriate or necessary to give full legal effect to this Section.

7. **CONFIDENTIALITY:**

7.1 **Mutual Exchange of Confidential Information.** The parties anticipate that each may disclose confidential information to the other. Accordingly, the parties desire to establish in this Section, terms governing the use and protection of certain information one party ("Owner") may disclose to the other party ("Recipient"). For purposes hereof, "Confidential Information" means information of an Owner:

(i) which relates to the purpose and subject matter of the Statement of Work, including computer programs, business/technical information, data, displays, recordings, images, and the like; or

(ii) which, although not related to the Statement of Work, is nevertheless disclosed hereunder, and which, in any case, is disclosed by an Owner or an affiliate to Recipient in document or other tangible form whether disclosed orally or visually and is identified as confidential; and

(iii) Confidential Information of KAISER includes, but is not limited to: financial data, personnel records, patient health information, patient records, medical records, computer programs, marketing information and any other information relating to the business affairs of KAISER.

7.2 **Non-Disclosure Obligations.**

7.2.1 Recipient may use Confidential Information of Owner only for the purposes of this Agreement and shall protect such Confidential Information from disclosure to others, using the same degree of care used to protect its own proprietary information of like importance, but in any case using no less than a reasonable degree of care.

7.2.2 Recipient may disclose Confidential Information received hereunder only as reasonably required to perform its obligations under this Agreement and only to its employees who have a need to know for such purposes and who are bound by signed, written agreements to protect the received Confidential Information from unauthorized use and disclosure.

7.2.3 The restrictions of this Agreement on use and disclosure of Confidential Information shall not apply to information:

(i) that is in the possession or control of Recipient prior to the time of its disclosure hereunder;

(ii) that is, or becomes publicly known, through no wrongful act of Recipient;

(iii) that is legally received by Recipient from a third party free to disclose it without obligation to Owner; or

(iv) that is independently developed by Recipient without reference to Confidential Information.

(v) after three (3) years from the date of execution of this Agreement, except as provided in Section 7.3, herein below.

7.3 **Recipient's Obligations.** As set forth under Section 7.2, above, the Recipient shall continue to hold, indefinitely, the Confidential Information described in Section 7.1 (iii), above.

8. **WARRANTY, DISCLAIMER AND LIMITATION OF LIABILITY:**

8.1 **Services.** SAFLINK hereby warrants and represents that the Services to be provided herein shall be performed in a good and workmanlike manner and consistent with generally accepted industry standards.

8.2 **Remedy.** For any breach of the above warranty, at KAISER'S sole discretion, remedy shall be provided for as follows:

(i) Require the timely re-performance of the Services as warranted and contained within the Statement of Work, and in the event that SAFLINK fails to re-perform the Services as stated herein, KAISER shall be entitled to recover all fees directly allocable to the defective Services paid to SAFLINK under the terms of this Agreement.

8.3 **Disclaimer.** EXCEPT FOR THE LIMITED WARRANTIES SET FORTH HEREIN, SAFLINK MAKES NO WARRANTIES, CONDITIONS OR REPRESENTATIONS WITH RESPECT TO THE SERVICES OR DELIVERABLES, WHETHER WRITTEN, ORAL, EXPRESS OR IMPLIED, IN FACT OR IN LAW, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES, CONDITIONS OR REPRESENTATIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OF DESIGN, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT, ALL OF WHICH ARE, TO THE EXTENT PERMISSIBLE BY LAW, HEREBY EXPRESSLY EXCLUDED AND DISCLAIMED.

8.4 **Limitation of Liability.** SAFLINK, ITS EMPLOYEES, AGENTS, OFFICERS, DIRECTORS, CONTRACTORS, CONSULTANTS AND/OR REPRESENTATIVES SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY, CONSEQUENTIAL LOSSES OR OTHER DAMAGES, WHETHER OR NOT THE POSSIBILITY OF SUCH LOSSES OR DAMAGES HAS BEEN DISCLOSED IN ADVANCE OR COULD HAVE BEEN REASONABLY FORESEEN. THE AGGREGATE LIABILITY OF SAFLINK, ITS EMPLOYEES, AGENTS, OFFICERS, DIRECTORS, CONTRACTORS, CONSULTANTS AND/OR REPRESENTATIVES, IF ANY, FOR ANY CLAIM OR LOSS ARISING OUT OF, OR CONNECTED WITH, THIS AGREEMENT, INCLUDING BREACH OF CONTRACT OR ANY EXPRESS OR IMPLIED WARRANTY OR CONDITION, NEGLIGENCE, USE OF THE SERVICES OR DELIVERABLES OR IF ANY REMEDY IS DEEMED TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, SHALL BE LIMITED SOLELY TO KAISER, AND SHALL NOT EXCEED THE AMOUNTS PAID TO SAFLINK BY KAISER FOR SUCH SERVICES OR DELIVERABLES, OR PARTS THEREOF, THAT DIRECTLY CAUSED SUCH LOSS OR DAMAGE.

8.5 **General Indemnity.** Subject to the other provisions of this Agreement, SAFLINK shall indemnify and hold harmless Kaiser, Kaiser Permanente Entities and their respective officers, agents, and affiliates from and against all liabilities, claims, losses, damages, demands and expenses, including reasonable attorneys' fees, arising out of or resulting from this Agreement to the extent that any such liabilities, claims, losses, damages, demands or expenses are caused by any act, error or omission of SAFLINK, its officers, employees, agents or consultants.

8.6 **Indemnity for Alleged Infringement.** SAFLINK warrants that it has the right to grant the license granted to Kaiser under this Agreement, free and clear of any liens and encumbrances, and that the Software and Deliverables will not infringe upon or violate any patent, copyright, trade secret, trademark, service mark, or other proprietary or intellectual property rights of any third party as of the date such Software or Deliverable is delivered to Kaiser ("Intellectual Property Rights"). SAFLINK shall indemnify, defend, save and hold harmless Kaiser, its respective officers, employees and agents from all claims, actions, losses, damages, liabilities, judgments, awards, costs and expenses, including reasonable attorneys', fees and costs, arising

out of claims that the Software infringes upon or violates Intellectual Property Rights of others. Kaiser shall promptly notify SAFLINK in writing if Kaiser becomes subject to any such claims. Kaiser shall, upon SAFLINK's request, at SAFLINK's expense and to the extent Kaiser's interests are not adverse to SAFLINK, provide reasonable assistance to SAFLINK in the defense of such action. SAFLINK shall have the sole control of the defense and settlement of such claims. If the Software becomes the subject of a claim of infringement or violation of the Intellectual Property Rights of a third party, SAFLINK may, at its sole option and expense:

(a) procure for Kaiser the right to continue using the Software; or

(b) replace or modify the Software so that no infringement or other violation of Intellectual Property Rights occurs, if Kaiser determines that:

(1) such replaced or modified Software will operate in all material respects in conformity with the then-current specifications for the Software; and

(2) Kaiser's use of the Software is uninterrupted and the performance of the Software is not impaired thereby. SAFLINK's obligations under this Agreement will continue with respect to the replaced or modified Software as if it were the original Software.

9. **TERM AND OBLIGATIONS:**

9.1 **Term.** The term of this Agreement shall commence immediately upon the date of execution by the parties hereinbelow, and shall continue in effect until the Statement of Work has been fully performed unless earlier terminated pursuant to Section 9.2.

9.2 **Termination.** Either party may terminate this Agreement if the other party breaches this Agreement (including without limitation the failure to make any payment when due) and the breaching party fails to cure such breach within thirty (30) days of the non-breaching party's written notice to the breaching party of such breach.

9.3 **Return of Materials.** Subject to the terms and conditions of any Statement of Work, or upon completion of any Statement of Work, either party may submit a written request to surrender all previously provided documentation, including, but not limited to, memoranda, notes, records, drawings, manuals, items or effects, whether tangible or intangible, of which were previously delivered by one party to the other. Furthermore, this provision shall apply to all materials made available or disclosed to either party by any third party source in connection with this Agreement or any Statement of Work.

9.4 **Continuing Obligations.** Sections 6, 7, 8, 9.3, 9.4 and 10.6 shall survive the expiration or termination of this Agreement for any reason.

10. **GENERAL:**

10.1 **Notices.** Except as otherwise provided, all notices hereunder shall be in writing and shall be deemed to have been received when:

(i) sent and received by facsimile transmission as indicated by a printed notice generated at the time of transmission;

(ii) mailed by certified mail, return receipt requested, postage prepaid, and properly addressed to the offices of the respective parties as specified in the introductory paragraph hereof, or at such address as the parties may later specify in writing for such purposes. The foregoing shall apply regardless of whether such mail is accepted or unclaimed.

10.2 **Merger; Amendment.** This Agreement shall not be considered an offer by either party, and it shall not be effective until executed by both parties. This Agreement constitutes and represents the entire understanding of the parties with respect to the subject matter of this Agreement and merges all respective prior communications, understandings, agreements, et al., hereunder. This Agreement may be modified and/or amended upon mutual agreement and written consent by the parties herein.

10.3 **Independent Contractors.** The relationship of the parties is that of independent contractor, and nothing herein shall be construed to create a partnership, joint venture, franchise, employment, or agency relationship between the parties.

10.4 **Severability.** If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law or public policy, the remaining provisions shall remain in full force and effect.

10.5 **No Implied Waivers.** The failure of either party to enforce at any time any of the provisions hereof shall not be a waiver of such provision, or any other provision, or of the right of such party thereafter to enforce any provision hereof.

10.6 **Governing Law.** This Agreement shall be construed under the laws of, and if required, adjudicated in the State of California, without regard to its principles or conflicts of law in any other jurisdiction.

10.7 **Multiple Counterparts.** This Agreement may be executed simultaneously in two or more counterparts, each one of which shall be deemed an original, but all of which shall constitute one and the same instrument.

10.8 **Assignment.** This Agreement shall inure to the benefit of, and be binding upon, any successor to all or substantially all of the business and assets of either party, whether by merger, sale of assets, or other agreements or operation of law. Except as provided herein, neither party shall assign this Agreement or any right or interest under this Agreement, nor delegate any work or obligation to be performed under this Agreement, without the other party's prior written consent. Any attempted assignment or delegation in contravention of this provision shall be void and ineffective and shall be deemed to be a material breach hereof. Notwithstanding any other provision of this Agreement, KAISER may assign this Agreement, to KAISER FOUNDATION HEALTH PLAN, INC., any of the PERMANENTE MEDICAL GROUPS or to:

(i) any parent, subsidiary, affiliated or successor corporation of KAISER; or the purchaser of any of these entities; or

(ii) any corporation to which KAISER has sold all or substantially all of its' assets (including the purchaser of any of KAISER's subsidiaries); and

(iii) any corporation or legal entity with which KAISER may merge or consolidate.

10.9 **Nondiscrimination and MediCare.** SAFLINK recognizes that as a governmental contractor, KAISER is subject to various federal laws, executive orders and regulations regarding equal opportunity and affirmative action which also may be applicable to subcontractors. SAFLINK, therefore, agrees that any and all applicable equal opportunity and affirmative action clauses from the **Federal Acquisition Regulation (*FAR*)** at **48 CFR Part 52** shall be incorporated herein by reference as required by federal laws, executive orders, and regulations, including, but not limited to the following ***FAR*** clauses:

(a) **Equal Opportunity** (Feb. 1999) at ***FAR* 52.222-26;**

(b) **Affirmative Action for Disabled Veterans of the Vietnam Era** (April, 1998) at ***FAR* 52.222-35;**

(c) **Affirmative Action for Workers with Disabilities** (June, 1998) at ***FAR* 52.222-36;**

(d) **Small Business Subcontracting Plan** (Oct. 1999) at ***FAR* 52.219-9.** If this agreement is determined to be subject to the provisions of **Section 952 of P.L. 96-499**, which governs access to books and records of subcontractors of services to Medicare providers where the cost of value of such services under the contract exceeds $10,000.00 over a 12-month period, then SAFLINK agrees to permit representatives of the Secretary of the Department of Health and Human Services and of the Comptroller General to have access to the contract and books, documents and records of SAFLINK, as necessary to verify the costs of the contract, in accordance with criteria and procedures contained in applicable Federal regulations.

10.10 **Advertising.** SAFLINK shall not, without the prior written consent of KAISER, use in advertising, publicity or otherwise, the name of KAISER FOUNDATION HEALTH PLAN, INC. or its subsidiaries, KAISER FOUNDATION HOSPITALS, any of the PERMANENTE MEDICAL GROUPS, KAISER PERMANENTE, or the KAISER PERMANENTE MEDICAL CARE PROGRAM, or refer to the existence of this Agreement in any press releases, advertising or materials distributed to prospective customers or other third parties, except that SAFLINK may use KAISER's name on its list of customers without obtaining the prior written consent of KAISER.

IN WITNESS WHEREOF, the parties have caused this Agreement to be duly executed below.

SAFLINK CORPORATION

By: Walt H. Hamilton

Title: V.P. BUSINESS DEVELOPMENT

KAISER FOUNDATION HOSPITALS

By: J Markel Jr

Title: DIRECTOR, TECHNOLOGY GROUP, NPO

EXHIBIT "A"
STATEMENT OF WORK

1. **DESCRIPTION OF WORK**: (Describe the Contracting Services, Deliverables, and delivery schedule.)

1.1 **Contracting Services**

The contracting services shown below include software development in accordance with the Requirements Specification and Functional Specification documents previously approved by the parties and included in this contract by reference. Requirements and capabilities indicated as "future" in these specification documents will be considered in the design of the pilot system, but will not be implemented as part of this contract.

Item #	Service	Period of Performance
1	Project Management	30 Aug 00- 30 Apr 01
2	Software Design	4 - 15 Sep 00
3	Software Development (code & unit test)	11 Sep - 31 Jan 01
4	Database Design & Development	11 Sep - 29 Sep 00
5	Integration Testing	2 Oct - 1 Dec 00
6	QA	16 Oct - 31 Jan 01
7	On-Site Test Support (up to 8 days)	23 Oct - 31 Jan 01
8	Documentation Development	23 Oct - 1 Dec 00
9	Training (Materials & Train-the-Trainer)	22 Nov - 31 Jan 01
10	Installation, Deployment, and On-Site Pilot Support (up to 6 days)	1 - 28 Feb 01 (nominal - 30 Apr 01)

Additionally, travel costs for up to eight (8) person-trips of up to 1 week's duration each have been included in the above statement of work. Any additional person trips will require contract modification and will be subject to additional cost.

1.2 **Deliverables and Delivery Schedule**

Item #	Item	Delivery Schedule
		Monthly
1	Project Status Reports	15 Oct 2000
2	Alpha software	15 Oct 2000
3	Biometric devices (I&T units) + SAFserver	1 Nov 2000
4	Beta software	15 Nov 2000
5	Beta 2 software	1 Dec 2000
6	Final software*	31 Jan 2001
7	Source code & updated executables	31 Jan 2001
8	Biometric devices (pilot units)	31 Jan 2001
9	User's manual(s)	31 Jan 2001
10	Training materials	

*Final software is subject to corrections required as a result of system testing.

Deliverable software includes the following configuration items (as described in the System Functional Specification):

- Authentication Administration App
- Authentication & Activation App
  Application Login Interface
- Badge Interface DLL (including badge SDK wrappers)
- Audit Logging App
- Key Management App

Software for the above includes all source code and executables, including any necessary configuration files (registry, ini, etc.), resource files, and data files. (This does not include the SAFLINK SAFserver™, which is separately deliverable under SAFLINK software license. See Exhibit B.)

EXHIBIT "B"
FIXED-FEE AND PAYMENT SCHEDULE

1. **FEES AND PAYMENT TERMS:**

1.1 Fees for the Services are charged on the basis of a guaranteed fee for the entire project described above which is $298,950.00.

1.2 Invoices for fees for the Services shall be billed and payable in accordance with the following schedule:

September 30, 2000	$100,000.00
November 30, 2000	$100,000.00
March 30, 2001	$ 98,950.00

Terms of payment will be net 30 days from date of invoice.

1.3 Non-services product items that may be required for the performance of this contract are not included in the above services fees. The prices for these items are included in the following schedule for reference purposes only and can be purchased through a separate purchase order.

Item	Quantity	Unit Price	Total
Software license for SAFLINK SAF2000 SAFserver™ component module (price is per user enrolled in SAFserver database)	25	$49.95	$1,248.75
Veridicom fingerprint sensor	5	129.00	645.00
Key Tronic fingerprint sensors	5	119.00	595.00
AuthenTec fingerprint sensors	5	129.00	645.00
IriScan SecureCam C2 iris camera	5	(TBD)	(TBD)
Total			$3,133.75

Note: Quantity discounts are available for subsequent system deployments.
Note: Above prices are valid for 30 days from the date of this Agreement.
Note: Biometric devices include hardware (device + cables), drivers, and Biometric Service Provider (BSP) modules.

Ver 1.2

SAFLINK CORPORATION

11417 Sunset Hills Road
Suite 106
Reston, VA 20190-5233

System Functional Specification

Biometric Authentication and Roaming Badge Technology Project

Prepared for

KAISER PERMANENTE

Kaiser Permanente
393 E. Walnut Street, 6th Floor
Pasadena, CA 91188

EXHIBIT B

Table of Contents

1.0 Introduction

1.1 Overview

Kaiser Permanente plans to implement an enhanced authentication capability for access to their Clinical Information System (CIS). This capability will involve the use of multiple technologies including biometrics, tokens, and PKI. The requirements for this authentication system are documented in the Biometric System Requirements Specification - Biometric Authentication and Roaming Badge (BARB) Technology Project.

1.2 Scope

This document defines the functional requirements for the enhanced CIS authentication system. The top down functional breakdown is graphically depicted in the form of data flow diagrams and textual descriptions.

Future requirements, when included, are indicated with dashed lines, square brackets [ ], or listed separately as future capabilities. These future requirements do not pertain to the pilot system implementation, but are included so that any implications for the overall system architecture and design can be considered.

The document is organized into the following sections:

Section 2 - Functional requirements
Section 3 - Operational sequence
Section 4 - Data elements
Section 5 - Security and availability features
Section 6 - Future requirements

2.0 Functional Requirements

The functional requirements for the enhanced CIS authentication (BARB) system are provided in this section.

2.1 Context

The context, or environment, that the authentication system will operate is depicted in Figure 1, below. This diagram identifies all external interfaces to the system, both human and other hardware/software elements.

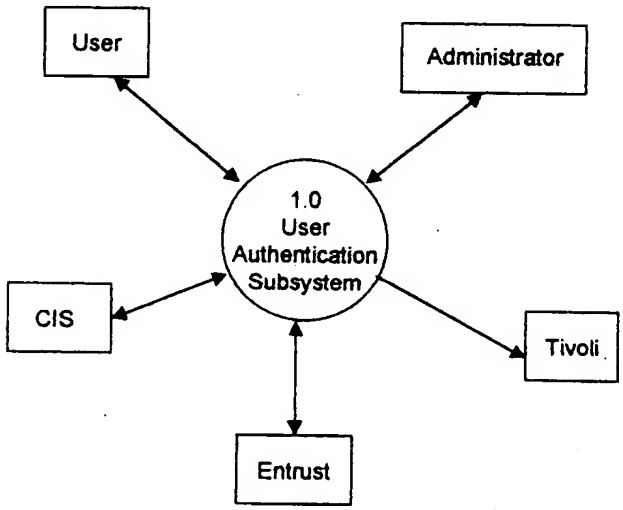


Figure 1. Context Diagram

These interfaces are briefly described below.

Administrator. The BARB subsystem administrator is the person authorized and responsible for system configuration, security, and user management.

User. Users are Kaiser staff personnel who need to access and use the CIS system in order to perform their job. This includes doctors, nurses, and other staff responsible for providing patient care.

CIS. The Clinical Information System (CIS) is the mission critical application for which the authentication system provides secure access.

Entrust. The Entrust system provides the public key infrastructure (PKI) upon which the user's access credentials are based. Entrust is accessed using the EntrustSession API.

Tivoli. This is an enterprise management system, which provides Application Resource Management (ARM) event logging and notifications.

Figure 2 depicts Kaiser's enhanced authentication system architecture.

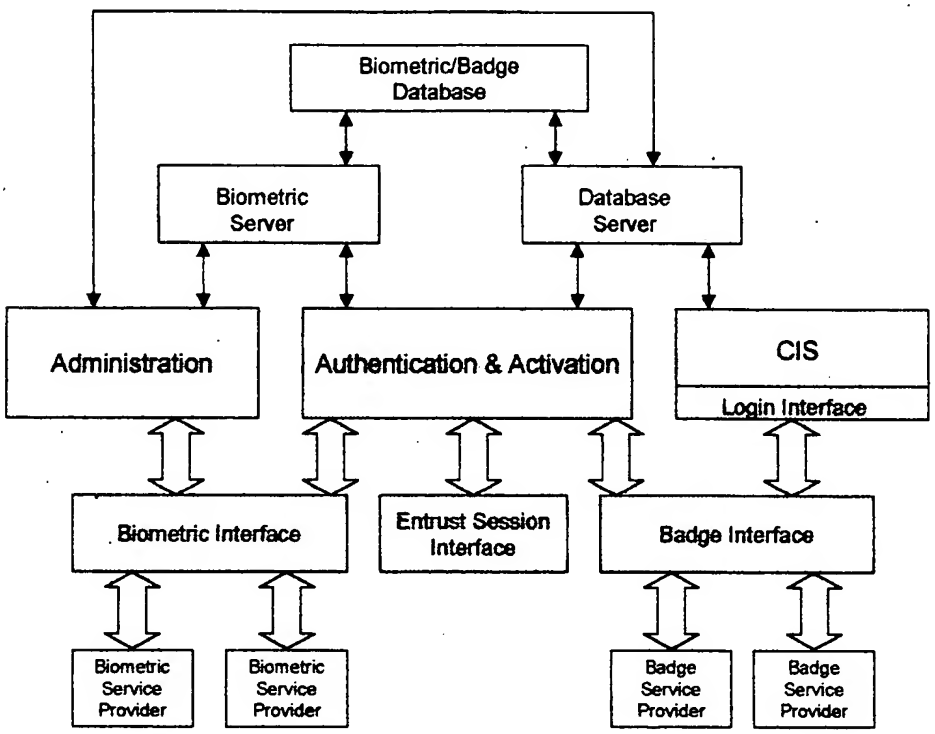


Figure 2. Kaiser Authentication Architecture.

2.2 System Functional Requirements

There are three primary functions performed by the user authentication subsystem. These are:

- Administration
- Authentication and Activation
- Application Login

Administration of the BARB subsystem is the process by which users' authentication information is maintained and authentication methods are managed, including enrollment of biometric characteristics and management of badge inventory.

Authentication and activation is the process by which a user is initially authenticated at the beginning of a shift and his badge is activated.

Application login verifies the identity of users and grants or denies them access to the CIS application at a given workstation.

Additionally, several supporting capabilities are provided.

Figure 3, below, depicts the top-level functional flow for the user authentication subsystem. In these data flow diagrams (DFDs), the "bubbles" represent system functions, the rectangles represent external elements, the pair of horizontal parallel lines represents data stores, and the arrows represent data (solid) or control (dashed) flow. No time sequence is implied in these diagrams (Section 3 addresses process flow).

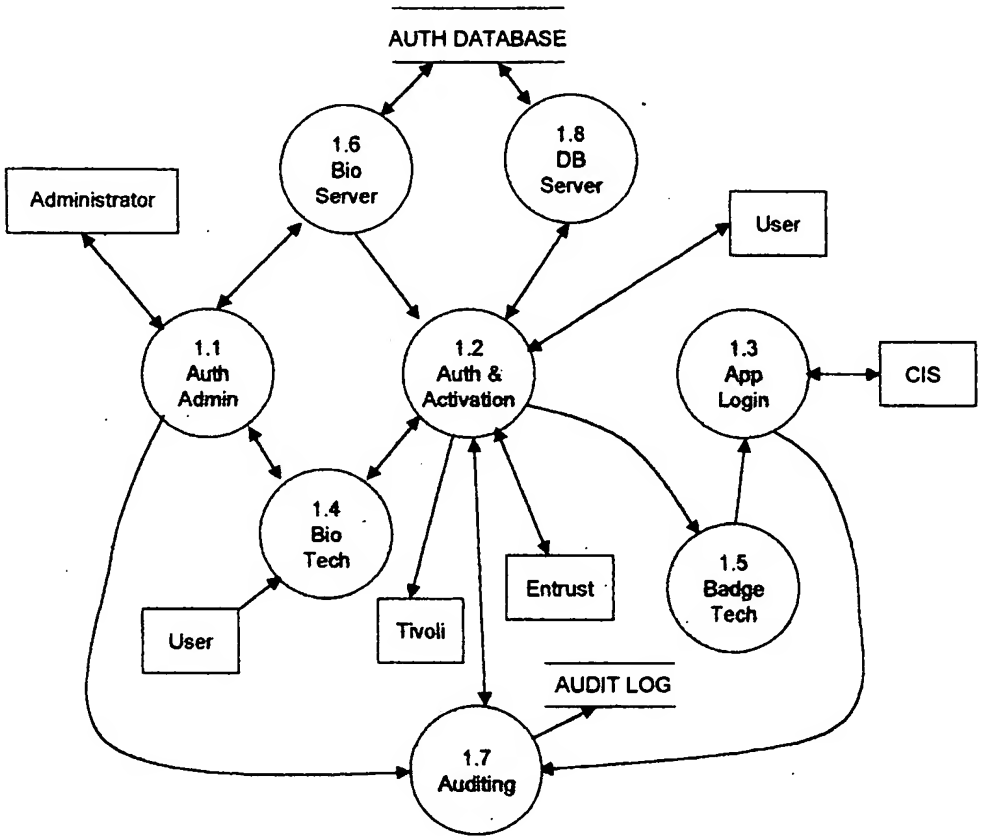


Figure 3. Top Level System Data Flow Diagram

NOTE: Use of the label "AUTH DATABASE" refers to both biometric and badge authentication data.

These functions are further described in the following paragraphs.

2.2.1 Authentication Administration

(1.1) abbr.

Authentication administration comprises one of three separate applications composing the BARB subsystem. It may run on a separate workstation or on the same workstation as the Authentication & Activation (A&A) application. Administration is the process by which users' authentication information is maintained and authentication methods are managed, including enrollment of biometric characteristics and management of badge inventory.

This function is composed of the following subfunctions, which are described in following subparagraphs. Each of these major functions should be accessible from the main/opening display page.

2.2.1.1 • User management

- Badge administration
- Biometric administration
- Access control (for the BARB subsystem administration functions)
- Administrator management (for the BARB subsystem administration functions)

The functional flow diagram for the authentication administration function is shown below in Figure 4.

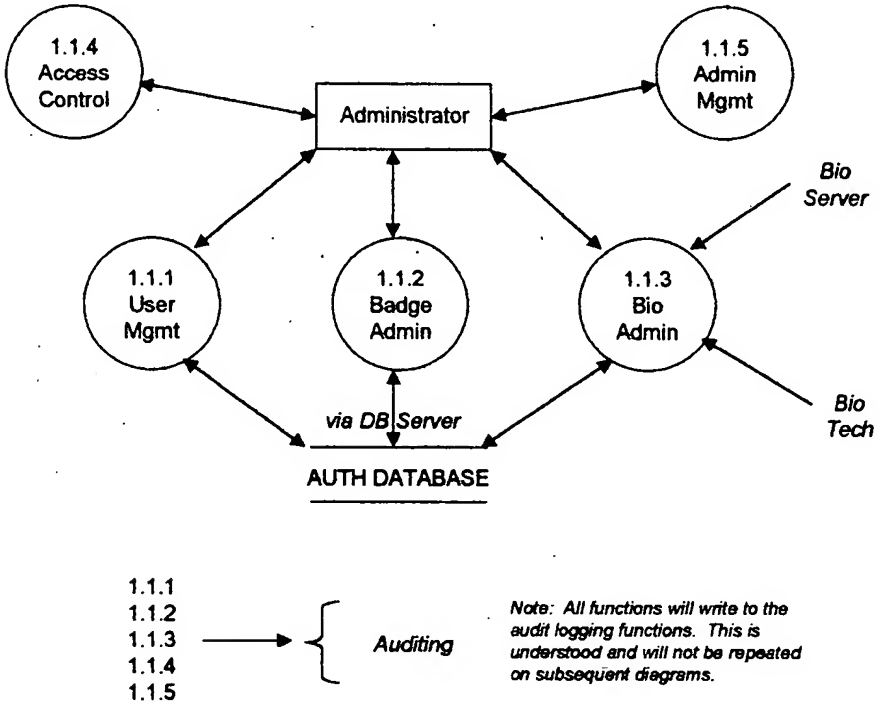


Figure 4. Authentication Administration Data Flow Diagram

Figure 5 depicts the general menu structure for the Authentication Administration application.

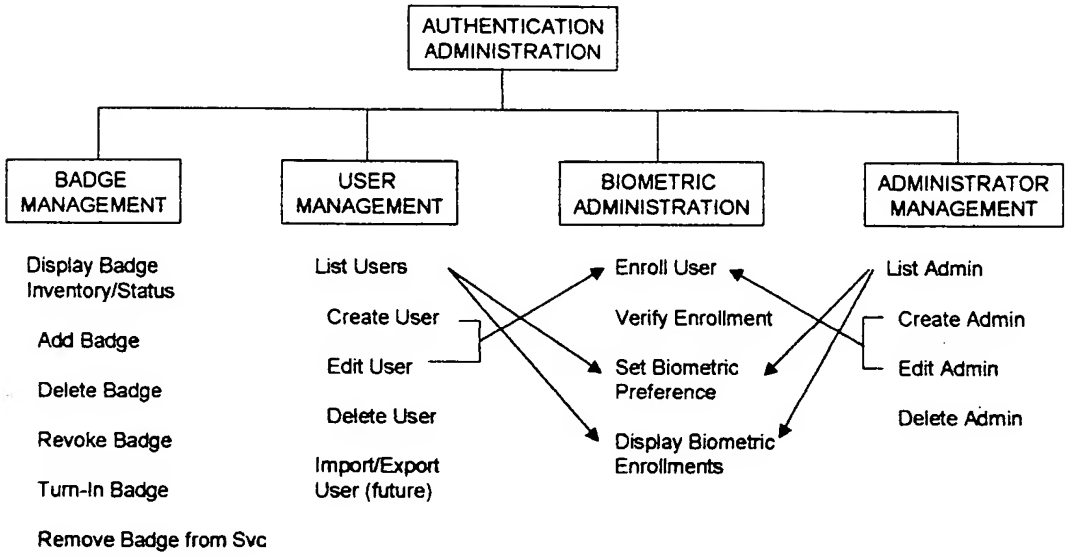


Figure 5. Authentication Administration Menu Structure

2.2.1.1 User Management

User management is the process by which user accounts are created and maintained within the authentication system, under the control of the system administrator. The user management function is accessed from the main/opening page of the administration application or via top level menu. User information is stored in tables within the authentication database (part of the biometric/badge database). The subfunctions composing user management include:

- List users
- Create user
- Delete user
- Edit user
- Import/export user (future)

The functional flow diagram for the user management function is shown below in Figure 6.

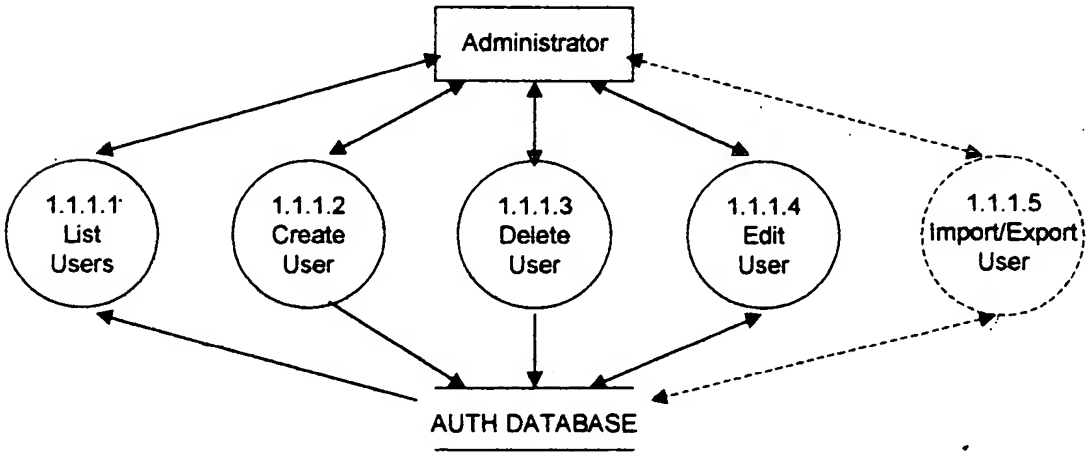


Figure 6. User Management Data Flow Diagram

2.2.1.1.1 List Users

When the "Users" tab is selected, the 'list users' function will display a list of registered system users, along with selected textual information associated with each user, in table format. By default, users will be listed in alphabetical order by user ID. By right-clicking in a different table column, the administrator can re-sort the user list based on the information in that column, alternating between ascending and descending modes. Double-clicking on a single user ID will invoke the 'Edit User' function (see below).

A font size of 12 points will be utilized in order to display the maximum amount of information that is easily readable. Vertical scrollbars will be provided to allow the administrator to view all users in the table; horizontal scrollbars will be provided to allow the viewing of all textual information about the users. Selecting another folder tab will close the 'list users' window.

2.2.1.1.2 Create User

This function will provide the capability to add new users to the authentication database. This function will be invoked via a pushbutton on the "Users" tab. Once invoked, a form will displayed into which the following information is to be entered:

User ID. A unique string value consisting of a beginning alpha character followed by 6 numeric characters. The User ID must be consistent with the user's Entrust User ID. This is a mandatory entry.

Last Name. The user's last name. Up to 35 alpha characters. This field may be left empty (null).

First Name. The user's first name. Up to 25 alpha characters. This field may be left empty (null).

Middle Initial. The user's middle initial. Single alpha character. If the user has no middle initial, this field is left blank (null).

Title. The user's title (such as Dr., Mrs., etc.), not job position. May be left blank (null). Up to 6 alpha characters.

Department. The user's department name or number. Up to 30 alphanumeric characters. This field may be left empty (null).

Phone Number. The user's office phone number. Separate fields will allow the administrator to enter the 3-digit area code, 3-digit exchange, 4-digit phone number, and up to a 5-digit extension. This field may be left empty (null).

Tie Line. The user's 3 character tie line prefix (numeric). This field may be left empty (null).

Email Address. The user's KP email address. Up to 48 text characters. This field may be left empty (null).

Badge Time-to-Live. The maximum time the user's badge will be activated before expiration. (Default is 12 hours.)

Additionally, from the 'create user' window, the administrator can initiate the 'enroll user' function (see 2.2.1.3.1) to enroll the biometrics of that user.

When all user information has been entered, the administrator may select via button 'Add User') to commit the new user information to the database. At this time, a validity check is made of the entered data to ensure that it meets data type and content specifications. The User ID is checked against the user database to ensure that it is unique. If all data is valid, the new user record is added to the user table of the authentication database and the "add user" window is closed-The user list will be updated to include the newly added user.

If any data is found to be invalid, the administrator is prompted to correct the entry. At any time prior to selecting OK/Save, the administrator may select to cancel or abort the new user creation process. If selected, a confirmation ("Are you sure?") will be required and if confirmed, any entered information will be discarded and the user information window closed.

Note: It would be prudent to verify that the User ID is valid before committing the transaction [this would require EntrustSession calls as used at the Activation Station]. While not absolutely required for the pilot, this would be mandatory for a post-pilot deployment. [Future]

2.2.1.1.3 Delete User

The administrator must have the capability to delete any user from the database. To do this, the administrator will highlight the user ID in the user list and either-select the 'Delete' button or press the 'Delete' key on the keyboard. If no user ID is highlighted when the 'delete user' function is selected, the administrator will be prompted to select a user ID. When the delete function is activated, the administrator will be asked to confirm ("Are you sure?") prior to deleting the user from the authentication database. A check will be made to ensure that the user identified for deletion exists within the database, in case another administrator almost simultaneously deleted that user from another workstation. When a user is deleted, all tables in the database associated with that user ID are deleted, including biometric tables. Once the user has been successfully deleted from the database, the administrator will be notified that the delete has been successfully completed and the user list will be updated to exclude the newly removed user.

Before deleting a user from the database, a check will be made to determine if any outstanding badges are assigned to that user (i.e, badge assignment status = assigned). If so, the administrator will be prompted with a list of assigned badges and given the opportunity to revoke these badges. An entry regarding this action will be made in the audit log.

2.2.1.1.4 Edit User

An existing user record may be updated using the 'edit user' function. This function will allow the administrator to change any user data except the user ID. To activate the 'edit user' function, the administrator may double-click on the user ID in the user list or may highlight the User ID and select the 'Properties' pushbutton. Upon activation, the same form as used for 'create user' will be displayed, with all fields containing the associated user data from the database. The UserID field will not be editable. The administrator may use the mouse, arrow, or tab keys to move from field to field and within fields to modify the contents of that field. From this window, the administrator may also choose to activate the 'enroll user' function to re-enroll (and thus update) the biometric data for that user. (Once the biometric enrollment is complete, control will return to the 'edit user' window.) Once all desired changes have been made to the user record, the administrator may select via the 'Update' button to commit the updated user information to the database, at which time the user information window is closed. If any data is found to be invalid, the administrator is prompted to correct the entry. At any time prior to this, the administrator may select to cancel or abort the 'edit user' process. If selected, a confirmation ("Are you sure?") will be required and if confirmed, any modified information will be discarded, no changes will be made to the database, and the user information window closed. Once the user data has been successfully updated in the database, the administrator will be notified that the update has been successfully completed.

2.2.1.2 Badge Administration

Badge administration is the process by which the inventory of badges is managed. This function is accessed from the main/opening page of the administration application or from a top-level menu. Badge information is stored in tables within the authentication database (part of the biometric/badge database). The subfunctions composing badge administration include:

- Display badge status
- Add badge
- Revoke badge
- Badge turn-in
- Remove badge from service

The functional flow diagram for the badge administration function is shown below in Figure 7.

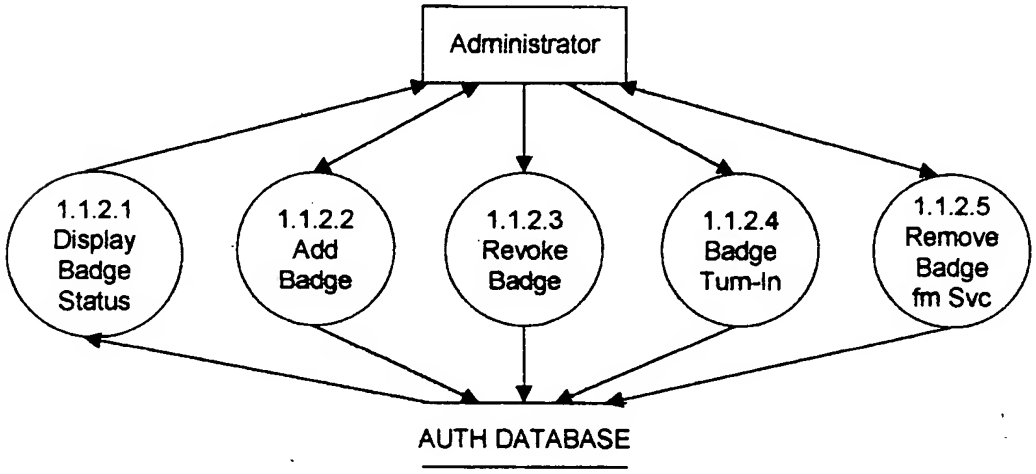


Figure 7. Badge Administration Data Flow Diagram

2.2.1.2.1 Display Badge Status

When the "Badges" tab is selected, the list of all badges in the inventory, along with current status information about that badge will be displayed in table format. By default, badges will be listed in alphabetical order by badge ID. By right-clicking in a different table column, the administrator can re-sort the badge list based on the information in that column, alternating between ascending and descending modes.

A font size of 12 points will be utilized in order to display the maximum amount of information that is easily readable. Vertical scrollbars will be provided to allow the administrator to view all badges in the table; horizontal scrollbars will be provided to allow the viewing of all textual information about the badges. Selecting another folder tab will close the 'list badges' window.

Information to be displayed includes the following:

Badge ID. The logical number of the badge as entered upon creation.
Badge serial number. The manufacturer's serial number of the badge [i.e. number "burned into badges memory"], entered upon creation.
Badge type. The type of badge technology (man-readable).

Badge assignment status. Current known status of the badge, either assigned, available, or out of service
Badge activation status. Activated, deactivated, revoked, or inactive.
User ID assigned. User ID of user most recently activating the badge.
Date/time of activation. Date and time of most recent activation.
Date/time of expiration. Date and time of expiration for most recent activation.
Last turn-in time. Date and time that badge was most recently returned.
Comment. An annotation that the administrator can apply to the badge.

The most probable use for the comment field would be to indicate why the badge was removed from service. Examples of such an annotation could be:

- Badge lost by "user name".
- Badge was returned to vendor for repair.
- Badge had hardware failure and was physically destroyed.

2.2.1.2.2 Add Badge

This function allows a badge to be added to the inventory of badges. This function will be invoked via a button on the "Badges" tab. When selected, a form will be displayed into which the administrator may enter the following information:

Badge ID. The badge ID is a logical ID that will be externally assigned and physically attached to the badge. Initially, this will be two numeric characters.
Badge Serial Number. This will be the manufacturer's serial number of the badge.
Badge Type. The administrator will select one of the available badge technologies which will be identified by an assigned value (e.g. "RFID" for RF Ideas, etc.).
Comment. An annotation that the administrator can apply to the badge.

Once the data has been entered, the administrator may select via the "Add Badge" button to commit the new badge information to the database. At this time, a validity check is made of the entered data to ensure that it meets data type and content specifications. Then a check is made of the badge database to ensure that the entered Badge ID is unique. If all data is valid, the badge information is added to the badge table of the authentication database and the "add badge" window is closed. In addition to the administrator-entered information, the remaining badge inventory status fields will be initially set as follows:

Badge assignment status. AVAILABLE.
Badge activation status. INACTIVE.

All other fields will remain unset (blank). When the "add badge" window closes, the badge status list will be updated to include the newly added badge.

If any data is found to be invalid, the administrator is prompted to correct the entry. At any time prior to selecting OK/Save, the administrator may select to cancel or abort the new badge creation process. If selected, a confirmation ("Are you sure?") will be required and if confirmed, any entered information will be discarded and the 'add badge' window closed.

2.2.1.2.3 Revoke Badge

This function allows the administrator to "revoke" or invalidate a badge (e.g. badge reported as lost or stolen, employee terminated, etc.). To do this, the administrator will highlight the badge ID on the badge status page (see 2.2.1.2.1) and select the 'Revoke Badge' button from the "Badges" tab. If no badge ID is highlighted when the revoke function is selected, the administrator will be prompted to select a badge ID When the 'revoke' function is activated, the administrator will be asked to confirm by manually typing the badge ID of the badge to be revoked prior to revoking the badge. The administrator may also make an entry in the comment field during the revocation process. When a badge is revoked, its activation status is changed to REVOKED in the authentication database, and reflected on the badge inventory status page.

At any time prior to confirming, the administrator may select to cancel the badge revocation process. Once a badge has been revoked, it may not be reinstated except through the 'badge turn in' process (see below).

2.2.1.2.4 Badge Turn In

At the end of the shift, users will turn-in their badges prior to leaving the facility for the day. As badges are turned in, the badge administrator will update the status of the badge in the badge database.

To do this, the administrator will highlight the badge ID on the badge status page (see 2.2.1.2.1) and select the 'Turn-in Badge' button from the "Badges" tab. If no badge ID is highlighted when the turn-in function is selected, the administrator will be prompted to select a badge ID. When the turn-in function is activated, a dialog box will appear for the administrator to manually type in the badge ID for confirmation, then select 'OK'. Once so confirmed, the status of the badge will be changed as follows (in the authentication database and reflected on the badge inventory status page):

Badge assignment status. Change to AVAILABLE.
Badge activation status. Change to INACTIVE.
Last turn-in time. Change to current date/time.

The administrator will also be provided the opportunity to make an entry in the comment field during the badge turn-in process.

The administrator may select 'CANCEL' to abort the badge turn-in operation prior to confirmation.

NOTE: This function is also used to reinstate a revoked badge or to return a badge to service that was previously removed.

2.2.1.2.5 Remove Badge from Service

This function allows the administrator to logically remove a badge from inventory. To do this, the administrator will highlight the badge ID on the badge status page (see 2.2.1.2.1) and select the "Remove Badge" button from the "Badges" tab. If no badge ID is highlighted when the 'remove badge from service' function is selected, the administrator will be prompted to select a badge ID. When this function is activated, the administrator will be asked to confirm by manually typing the badge ID number prior to removing the badge from service by updating the badge tables in the authentication database. The administrator will be provided the opportunity to update the comment field. When a badge is removed, its status will be changed as follows:

Badge assignment status. Change to REMOVED FROM SERVICE.
Badge activation status. Change to INACTIVE.
Last turn-in time. Change to current date/time.

Once the badge has been successfully removed, the badge inventory status list will be updated.

2.2.1.3 Biometric Administration

Biometric administration is the process by which users' biometric data is enrolled into the system. Biometric information is stored in tables within the authentication database (part of the biometric/badge database). This function is accessed from a button on the user/administrator property page. The subfunctions composing biometric administration include:

- Enroll user
- Store template
- Set biometric preference
- Display biometric enrollments
- Verify biometric enrollment

The functional flow diagram for the badge administration function is shown below in Figure 8.

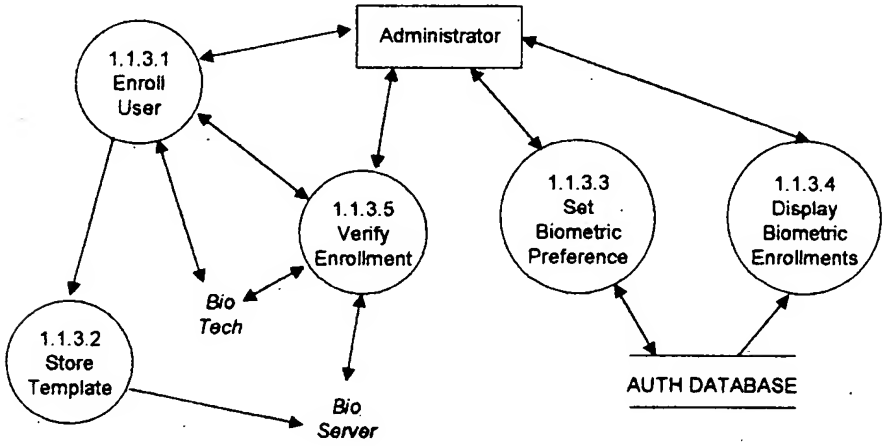


Figure 8. Biometric Administration Data Flow Diagram

2.2.1.3.1 Enroll User

Enrollment is the process by which a user's biometric information is captured and processed for storage and future matching. This function is activated from the 'Create Admin', 'Edit Admin', 'Create User' or 'Edit User' functions, by highlighting the user ID on the user/admin list and selecting the 'Properties' button, then the 'Enroll' button.

Upon selection, the administrator will be provided a choice of biometrics to be enrolled, from those that are available (i.e., installed on the system). The administrator may select one biometric at a time in which to enroll a given user. Upon selection, the application will invoke the enrollment function of the selected biometric technology via the HA-API interface. This will result in the return of the biometric identifier record (BIR), also known as a template, or a cancellation (e.g. enrollment function failed or was cancelled by user).

If a valid BIR is received, it will be sent (along with the User ID) to the Store Template function (see below). If a cancellation is received, the screen will return to the initial biometric enrollment/select biometric window. The administrator may then enroll the user in another biometric, if desired, or exit the function.

2.2.1.3.2 Store Template

Upon receipt of a valid BIR and user ID from the 'enroll user' function, the 'store template' function will package this information for submission to the Biometric Server. This will be accomplished via the client interface component of the Biometric Server, which resides on the workstation. Client/server communications will be via a secure RPC channel using existing OS utilities/services.

This function will then update the user record within the authentication database to indicate that the user has been enrolled in the particular biometric technology. This is tracked by the BUID number of the HA-API BSP. If no other biometrics have thus far been enrolled, the currently stored biometric will also be entered as the preferred biometric.

2.2.1.3.3 Set Biometric Preference

Once the Biometric Enrollment dialog is displayed for the current user ID or admin ID, the administrator can change the biometric preference by selecting a biometric method from the list box and hitting the "Set Preference" button. The user/admin must have already been enrolled via the selected method, as indicated by a checkmark. If no checkmarked method is highlighted when the 'Set Preference' function is selected, the administrator will be prompted to select a method. Otherwise, the selected method will be displayed in the preferred biometric field below the user/admin ID.

At any time prior to selecting OK/Save, the administrator may select to cancel or abort the biometric enrollment process. If selected, a confirmation ("Are you sure?") will be required and if confirmed, any entered information will be discarded and the 'biometric enrollment' window closed.

2.2.1.3.4 Display Biometric Enrollments

This function will display, for a given user, the biometrics in which the user has been enrolled along with the preferred biometric. This function will be invoked when the administrator selects the 'Enroll' button from the User/Administrator properties page. From this window, the administrator will also be able to invoke the Enroll User (2.2.1.3.1) and Set Biometric Preference (2.2.1.3.3) functions.

When the list of biometric enrollments is displayed, the preferred biometric will be indicated (either by a separate listing or via highlighting). Any enrolled biometrics for which the matching technology is not installed on the admin workstation will be grayed out to indicate non-availability for re-enrollment at that station. If other available biometric technologies are listed (to enable selection for enrollment), then the enrolled biometrics will be distinguished from un-enrolled biometrics by a checkmark or other clear indicator.

2.2.1.3.5 Verify Biometric Enrollment

From the Display Biometrics window, the administrator may select to verify a user biometric enrollment. The administrator may select any enrolled, available technology from the biometrics list and invoke the Verify Biometric Enrollment function by pressing the "Verify" button.

Upon activation the selected biometric technology will be activated to perform a local biometric capture and processing operation, followed by a server verify operation. The results of the verify will be displayed (i.e., Match or No Match). The administrator may then choose to close this window and return to the Display Biometrics window.

This function is provided in order to check the quality of a biometric enrollment to ensure the template is matchable by the user immediately following the enrollment process while the user is still available. However, the function may also be used at other times – for example, if the user has been experiencing trouble authenticating at the A&A station with a particular biometric technology.

2.2.1.4 Administrator Management

Administrators are those individuals authorized to access the Authentication Administration application and perform the above functions. They are the system operators. Functions must be available to manage the list of authorized administrators and their associated data.

This function consists of the same functions as user management (described in 2.2.1.1) and uses the biometric enrollment and display biometric enrollment functions described in 2.2.1.3. The only differences are that no biometric preference is associated with an administrator (they may log-in with any enrolled/installed biometric), no import/export function exists, and there is an additional password capability associated with administrators.

2.2.1.5 BARB Access Control

This function controls access to the BARB Administrator Application. Upon launch and initialization of this application, the administrator will be asked to biometrically authenticate themselves before the access to administrative functions are granted.

When the BARB Administrator Application, the administrator's access will be restricted to the "Login" Tab and menu help functions. On the "Login" dialog, the administrator will type his/her identifier into the 'Admin ID' field in the "Login" tab window, may enter the backup password into the password field, and will select the "Login" button (or depress the ENTER button). If the Admin ID doesn't match any stored IDs in the database, the administrator will be informed of such and the fields cleared for further attempts.

If the Admin ID is found and no password was typed in, then the application will invoke the verification function of the selected biometric technology via the HA-API interface. Is the acquired biometric matches the stored biometric, the administrator will be informed of the match and will be granted access to the other areas of the dialog.

If a password was provided, then it will be checked against the backup password currently assigned to that Admin ID. If they match, the administrator will be informed of the match and will be granted access to the other areas of the dialog.

A logout function is provided to allow one administrator to logout so that another administrator can log in without closing the program. When an administrator selects the "Logout" button, the application will prompt "Are you sure you want to logout?". If he selects "Yes", then the "Badges", "Users", and "Admins" tabs will be locked down; an asterisk is added to the tab as a reminder.

2.2.2 Authentication and Activation

Authentication and activation (A&A) comprises one of three separate applications composing the authentication subsystem. It may run on a separate workstation or on the same workstation as the 'authentication administration' application. Authentication is the process by which a user's identity is verified at the beginning of each shift, prior to badge activation. Activation is the process by which the user's authentication credentials are uploaded to the badge and the badge is activated for some preset amount of time.

This function is composed of the following subfunctions, which are described in the following subparagraphs.

- Validate badge
- Check credentials
- Biometric authentication
- Activate badge
- A&A utilities

The functional flow diagram for the authentication and activation function is shown below in Figure 9.

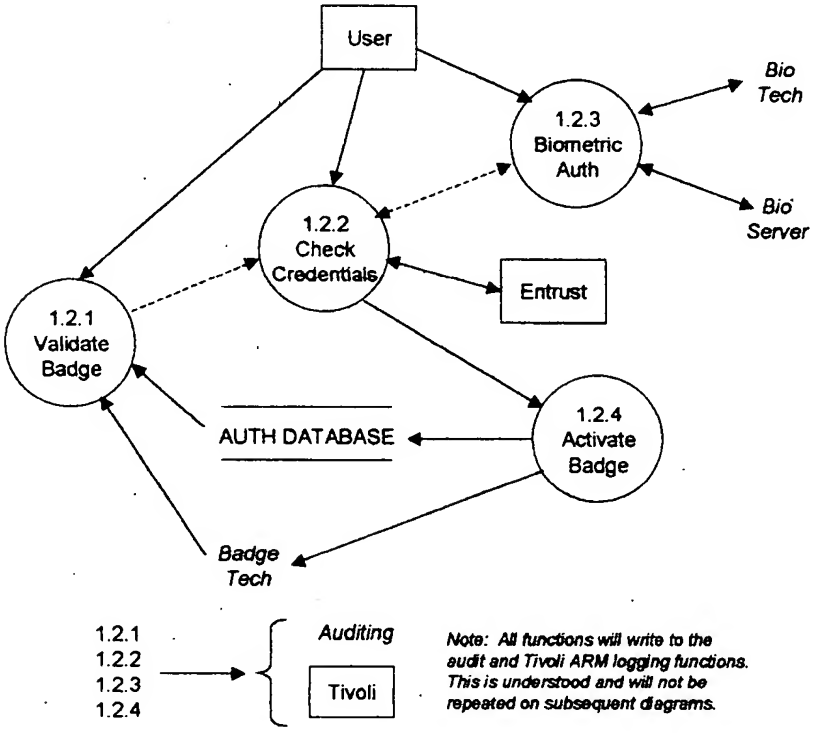


Figure 9. Data Flow Diagram for Authentication and Activation Application

Note that prior to approaching the authentication and activation station, the user should have picked up an inactive badge from the inventory of badges. This badge must be present in order to be activated.

When the authentication and activation application is initiated, a main display screen will be presented. Options available on this page will include:

- Activate badge (default)
- Options
  - Activate badge with password change
  - Deactivate badge

Also, when the application is first initialized, it will retrieve from the Key Holder (ancillary function), the crypto key for encrypting/decrypting badge data.

Upon initialization, and thereafter, the badge technology function will (unsolicited) provide a badge state table to the A&A function. This table will be refreshed each time a change in state occurs (badge detected, badge no longer present, change in badge status).

2.2.2.1 Validate Badge

This function is initiated upon completion of program initialization (i.e., upon launch). The system will prompt the user to enter the logical badge number of the badge to be activated, the user ID, and password, as shown below:

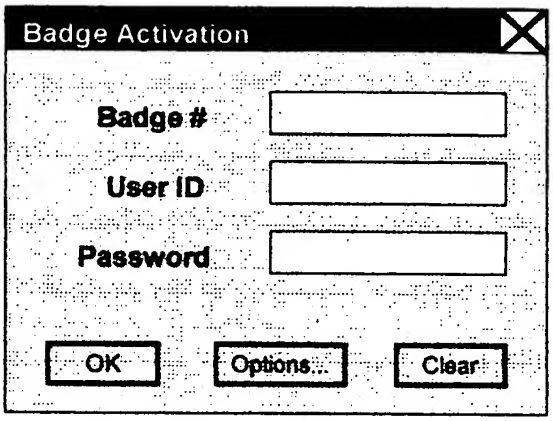


Figure 10. Badge Activation Window

The user will enter data into all fields, then press 'OK' or the "Enter/Return" key when done. The 'Tab' key will move the cursor between fields, or the mouse may be used to position the cursor, which will default initially to the Badge # entry box. The Badge number and User ID will be displayed as typed; however, the password characters will only be displayed as asterisks.

NOTE: If at any time during the badge activation process, the process is discontinued for any reason, the entered password data will be purged from memory.

Upon receipt of this entry ('OK' is pressed), the A&A application will query the authentication database to:

a. Check to see if the entered logical badge ID exists. If the entered logical badge ID does not exist, an error message will be displayed to the operator.
b. Retrieve the manufacturer serial number associated with the entered logical badge ID from the Authentication/Badge database.

It will then retrieve the current badge state table to see if the serial number for the entered badge ID is present (via the Badge Technology function). This query should return badge serial numbers for either one badge, multiple badges, or no badges.

If no serial numbers are returned, the user will be prompted to position the badge for proper reading and the badge query will be retried. After a preset timeout period (see INI file), the user will be prompted to return the badge to the administrator and check out another badge and the application will return to the main screen (clearing all entries, and purging the entered password from memory). If upon repositioning, a serial number is returned, then processing will continue as shown in the following paragraph.

If only one serial number is returned, then the authentication database will be queried for the status of that badge. The result of this query should be the data listed in Section 2.2.1.2.1. A check will be made that the logical badge number entered matches that from inventory. If not, or if the logical badge number does not exist in the inventory, the user will be asked to re-enter the logical badge number. If it now matches, processing will proceed. Otherwise, this will be repeated until the user has entered up to 3 logical serial numbers without success. At this point, the application will display an error message (asking the user to return this badge to the badge return area and select another) and return to and clear the main screen.

If multiple serial numbers are returned, then the A&A application will query the authentication database for the status of the logical badge number entered by the user. If the serial number returned from the inventory database matches one of the serial numbers present, then it will be assumed that this is the badge to be activated and processing will proceed. If the returned serial number does not match any present, or if the logical badge number does not exist in the inventory, the user will be asked to reenter the logical badge number, which will then be queried for status from the inventory and matched against serial numbers present. This will be repeated until the user has entered up to 3 logical serial numbers without success, at which point the user will be prompted to return the badge to the administrator and check out another badge. The application will return to and clear the main screen.

The second check (of the badge inventory status information) will be of the badge assignment status field. If this field reflects 'available', then processing will continue. If the badge status = "assigned" or "out of service", the user will be prompted to return this badge to the administrator and select another, and the application will return to the main screen.

The third check (of the badge inventory status information) will be of the badge activation status field. If this field reflects 'inactive', then processing will continue. If the badge activation status = 'activated' or 'deactivated', then this indicates an unreturned badge. In this case, the user will be prompted to return the badge to the administrator and check out another badge. If the badge activation status = 'revoked', then the user will be prompted to return the badge to the administrator and check out another badge.

Next, the badge will be queried for its status (via the badge technology function). The A&A function will query the user's badge (with the serial number matching the logical serial number entered) for badge status. If enabled (check INI file), it will check battery status to determine that the battery is adequately charged (i.e., exceeds minimum value in INI file). If so, processing will continue. If not, the user will be prompted to return the badge to the badge return area and select another, with the application returning to and clearing the main screen.

If the battery check passes, then a check will be made to determine if the badge is ready for activation. This involves determining if the badge is located on the user's person and if the KP ID badge is inserted (by checking the badge state table). The INI file is first checked to determine which badge checks are enabled. Then the status bits are checked. The table below provides a delineation of the actions to be taken depending on these factors.

ENABLED?	On-person	T				T				F				F			
	KP-ID	T				F				T				F			
VALID?	On-person	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
	KP-ID	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
ACTION		A	B	C	D	A	A	C	C	A	B	A	B	A	A	A	A

A = Processing continues
B = User is prompted to insert KPID into badge; KPID checks continue until good or timeout
C = User is prompted to attach badge to person; On-person checks continue until good or timeout
D = User is prompted to insert KPID into badge and attach badge to person; checks continue until both values are good.

Figure 11. Badge Ready Check Table

If a check is enabled (T), but the associated value is found to be invalid (0), the user will be prompted to take the appropriate action to correct the condition. The faulty indicator will be continuously checked until the status changes to 'yes' (1) or until a preset 'badge check timeout' period (defined in the INI file) has expired. After the timeout expires, the user will be prompted to return the badge to the administrator and check out another and the application will return to the main screen.

If the badge passes all validation checks (serial number matches logical badge number, badge is available, badge is inactive, battery is OK, badge is on-person, and ID is inserted), then control will pass to the Check Credentials function (see below).

2.2.2.2 Check Credentials

Once it has been determined that a valid badge is present, then the user's credentials will be checked. A dialog box will be presented letting the user know his credentials are being verified ("Verifying Password"). Previously (see 2.2.2.1), a window will have been displayed asking the user to enter their CIS/Entrust User ID and Password. Once 'OK' or 'Enter' has been pressed, a validity check will be performed to determine that a) both fields contain data and that b) the entered data is of the correct format (as defined in Entrust API). If either field is invalid, the user will be prompted to re-enter them. If both fields are valid, then the following processing will be performed:

a) The entered User ID and password will be submitted to Entrust (external interface using EntrustSession API) for a credential check. If the credential check is successful, then step b) will be performed. If the credential check is unsuccessful, then the user will be prompted to reenter the User ID and Password. Three tries will be permitted. After three unsuccessful attempts, the user will be prompted to contact the system administrator and the application will return to the main screen. [Entrust may do user lockout.]
b) The entered User ID will be checked against the Authentication database to ensure that it exists. If so, the user record associated with the entered User ID will be retrieved from the authentication database (for subsequent processing) and step c) will be performed. If not, the user will be prompted to contact the system administrator and the application will return to the main screen.
c) The authentication database will be searched to determine if any active, unexpired badges are already assigned to the entered User ID. If not, processing will continue to step d). If so, the user will be prompted that he already had another active badge and to see the system administrator, with the application returning to the main screen.
d) The authentication database will then be searched to determine if any inactive, unreturned badges are assigned to the entered User ID. If not, processing will continue. If so, and the number is less than the maximum permitted (defined in INI file), the user will be prompted

that he has X number of unreturned badges and to please return them to the badge return area as soon as possible. Processing will then continue and control will pass to the Biometric Authentication function (below). If so, and the number meets or exceeds the maximum permitted (defined in the INI file), the user will be prompted that he has exceeded his number of assigned badges and must see the system administrator to resolve the issue prior to any additional badge activations. In this case, the application will return to the main screen.

If after a successful credential check Entrust returns a mandatory password change, see 2.2.2.5.2.

2.2.2.3 Biometric Authentication

Once the user's credentials have been validated, biometric authentication will be performed to ensure that the user is who he claims to be. The biometric authentication process consists of the following four subfunctions:

- Biometric selection
- Capture biometric
- Process biometric
- Verify biometric

Figure 12, below, is the DFD for the biometric authentication function.

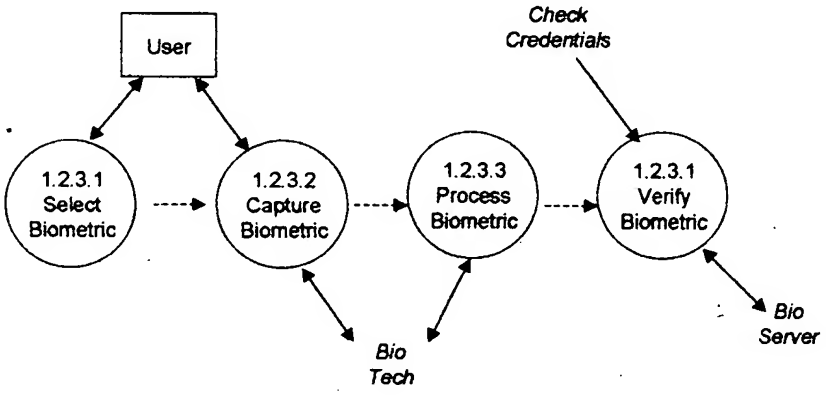


Figure 12. Biometric Authentication Data Flow Diagram

2.2.2.3.1 Select Biometric

Once the user's credentials have been validated, the user record (from 2.2.2.2.b, above) will be checked to determine that the user has been biometrically enrolled, which biometric technologies have been enrolled, and what is the preferred biometric.

If no biometrics have been enrolled, the user will be prompted that he is not yet biometrically enrolled and he should see the system administrator for information regarding enrollment. The application will then return to the main screen.

If one or more biometric enrollments exist, a check will be made to ensure that the preferred biometric is installed on the A&A station. If not, the next enrolled biometrics will be checked in sequence until an installed biometric technology is found or until the list is exhausted. If none of the enrolled biometrics is installed, a message will be displayed to the user indicating that none of his enrolled biometric

technologies are available and to contact the system administrator for assistance, with the application returning to the main screen.

If the preferred biometric (or a subsequent enrolled biometric) is installed, then the A&A application will initiate a biometric capture (below), passing it the Biometric Unique ID (BUID) of the biometric technology to be used.

2.2.2.3.2 Capture Biometric

Via the Biometric Technology interface, this function will initiate a capture of the user's raw biometric data sample using the selected biometric technology BSP/device. This will return either a raw BIR or a cancellation. If a raw BIR is returned, then it will be forwarded to the Process Biometric function (below) for processing. If the function is cancelled, the user will be queried to choose either to a) retry current biometric type, b) try other biometric type [assuming the user is enrolled in the other biometric type], or c) abort activation, as shown in Figure 13, below.

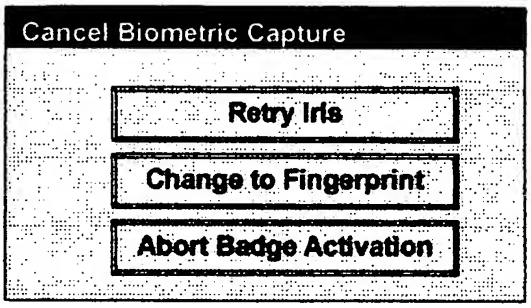


Figure 13. Cancel Biometric Capture Window.

If the user selects "Retry xxxxx", then the capture will be reinitiated. If the user selects "Change to yyyyy", then a capture will be initiated for the next enrolled biometric technology of the opposite type (e.g., if the user initially attempted an iris verification, a biometric capture of the next enrolled fingerprint technology that is installed will be initiated). An unlimited number of captures will be allowed. Once selected, the biometric capture will be reinitiated for the selected technology. If the user selects "Abort Badge Activation", then after a confirmation ("Are you sure?"), the application will return to the main screen.

Note: The biometric capture is performed locally on the A&A station.

2.2.2.3.3 Process Biometric

Upon receipt of a valid raw BIR, this function will initiate processing of the user's raw BIR into a processed BIR, suitable for subsequent matching. This is done via the Biometric Technology interface to the selected BSP, which will return a processed BIR. This processed BIR will then be forwarded to the Verify Biometric function (below) for verification matching.

Note: Biometric processing is performed locally on the A&A station.

2.2.2.3.4 Verify Biometric

Upon receipt of a BUID, processed BIR, and User ID, this function will initiate a 1:1 verification match via the Biometric Server function. This will be accomplished via the client interface component of

the Biometric Server, which resides on the workstation. Client/server communications will be via a secure RPC channel using existing OS utilities/services.

The Biometric Server will return the results of the verification match as either a 'match' or 'no-match'. If the results are 'match', then the user's identity has been successfully verified and processing will continue to the Activate Badge function (below). If the results are 'no-match', the user will be notified via a message box that the verification failed. He will be then given the option to "Retry xxxxx" or "Change to yyyyy" to try again with a different biometric, or "Abort Badge Activation"(See Figure 13).

If the user elects to try again, the Capture Biometric function will be reinitiated. If the user elects to try again with a different biometric type, then a capture will be initiated for the next enrolled biometric technology of the opposite type (e.g., if the user initially attempted an iris verification, a biometric capture of the next enrolled fingerprint technology will be initiated). An unlimited number of retries will be allowed, but each attempt will be recorded in the audit log (see 2.2.7).

If the user elects to abort activation, the application will return to the main screen.

2.2.2.4 Activate Badge

This function is activated upon completion of a successful biometric authentication. At this point, the A&A application has data regarding the valid badge, the user, and the users credentials. The data flow diagram for this function is shown in Figure 14, below.

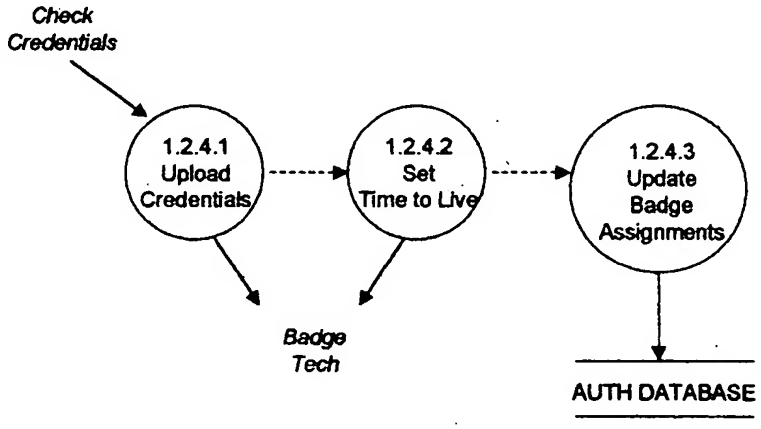


Figure 14. Activate Badge Data Flow Diagram

First, the badge status must be re-checked to ensure that the badge is ready for activation. This information is obtained by querying the Badge Technology interface for the serial number of interest. Upon receipt of the badge status information, the following will be checked:

- Badge is still present.
- Badge is 'on-person' (if check is enabled, INI file setting for specific badge technology)
- KP picture ID is inserted (if check is enabled, INI file setting for specific badge technology)

If the badge is not present, the user will be prompted to position the badge for writing, and the badge query will be retried. After a preset timeout period (see INI file), the user will be prompted to return the badge to the administrator and check out another badge and the application will return to the main screen (clearing all entries). If upon repositioning, badge presence is detected, then processing will continue as shown in the following paragraph.

If the badge is present, the 'on-person' and KPID fields will be checked, if checking is enabled for the badge technology. This is performed in the same manner as described in 2.2.2.1.

Once all three conditions are met, the Upload Credentials function will be activated.

2.2.2.4.1 Upload Credentials

When the badge has been confirmed as 'ready to write,' a badge write will be issued to the Badge Technology interface. Three actions will be performed:

- Reset badge
- Initialize badge
- Write user credentials

First, the badge will be reset, which should bring it to some known, initial (power-up) state. This involves resetting the following:

- Reset 'on-person confidence' to 100%
- Reset 'KPID ever removed' to No/False
- Set broadcast back-off interval (number of interval units)

Second, the badge will be initialized. This will include setting of the global password.

Then the following user credentials will be encrypted (using the encryption key obtained from the key holder, 2.2.81, during start-up) and written to the badge via the badge interface, which handles the security associated with the badge:

User ID: tag = "UID", data = annnnnn, password = global PW
User password: tag = "UPW", data = up to 16 alphanumeric characters, password = global PW

Note - for the pilot, the global password will be hardcoded into the application and the field passwords will be the same as the global passwords.

Note: User data is encrypted by the BARB subsystem before writing to the badge.

2.2.2.4.2 Set Time-to-Live/ Activate Badge

In addition to the user's credentials, two other writes to the badge must be performed:

- Time-to-live
- Activate badge

The time-to-live value is associated with a specific user and will have previously been retrieved with the user record from the authentication database (see 2.2.2.2.b). This value will be written to the badge, via the Badge Technology badge interface as follows:

Time-to-live: tag = "TTL", data = nn (hours), password = global PW

Note that depending on technology, this data may require conversion into an expiration date/time group and may be done in terms of a command rather than a data field.

Once all pertinent data has been successfully written to the badge, the badge is 'activated' (set to active). Once activated, all user credentials will be purged from memory (zeroed out).

2.2.2.4.3 Update Badge Assignments

Upon successful badge activation, a message will be displayed to the user showing:

- "Activation Successful"
- User name
- User ID
- Logical badge number
- Expiration date and time

In addition, badge status in the authentication database is updated as follows:

Badge ID. No change (not writable by this application)
Badge serial number. No change (not writable by this application)
Badge assignment status. ASSIGNED
Badge activation status. ACTIVE
User ID assigned. USER ID
Date/time of activation. ACTIVATION DTG
Date/time of expiration. EXPIRATION DTG
Last turn-in time. No change (not writable by this application)

2.2.2.5 Activate Badge with Password Change

The user's password may be changed in two ways: a) user initiated (on-demand) password change or b) Entrust initiated (periodic) password change. The processing for these two situations is described in the following subparagraphs.

In either event, the user will go through the normal badge activation sequence described in sections 2.2.2.1 - 2.2.2.4, above, except as follows. Prior to activating the Upload Credentials function (step 2.2.2.4.1), the Change Password function described in 2.2.2.5.1 or 2.2.2.5.2, below, will be performed as a modification of step 2.2.2.2.a.

2.2.2.5.1 Change Password

This function provides the capability for a user initiated CIS/Entrust password change. It is initiated by selecting 'Options' from the main screen (see Figure 10), which brings up the following window:

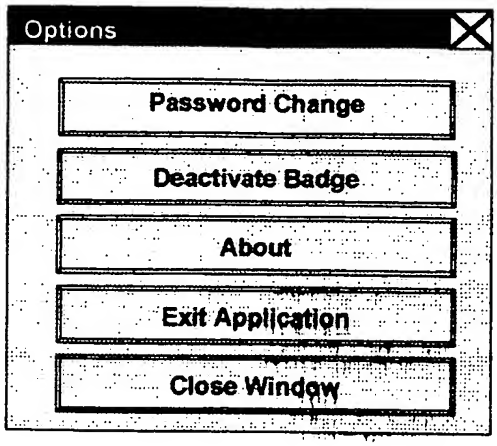


Figure 15. Options Window

When the 'Password Change' option is selected from the main screen, the following window will be presented.

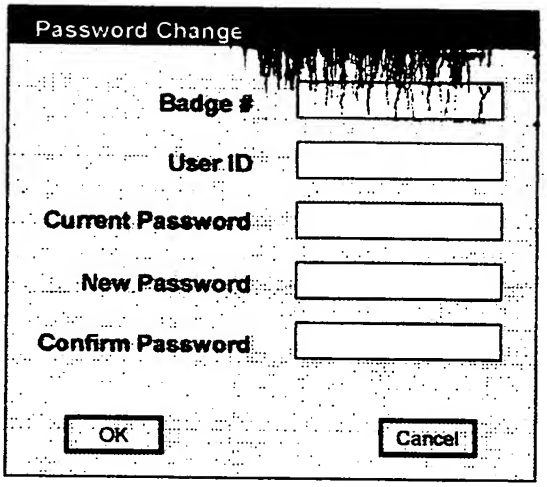


Figure 16. Password Change Window

The user will be asked to enter their badge number, user ID, and password, as normally done in 2.2.2.1. The user will also be asked to enter the new password twice. If the new and confirm passwords are not identical, an error message will be displayed and the user asked to reenter the new/confirm passwords.

The rules for password selection should be displayed at this time. These are:

- The new password must be at least eight characters long, but not more than 16 characters
- No particular character may make up more than half the characters in the new password
- The new password may contain no more than 2 consecutive repeating characters.
- The new password may not begin or end with a numeric.
- The new password cannot contain the name of the user's profile
- The name of the user may not make up more than half of the password
- The new password must contain at least one lowercase letter and one uppercase letter
- The new password may not be the same as the old password

- The new password may not contain more than 3 consecutive identical characters in common with the old password.

The user will enter data into all five fields, then press 'OK' or the "Enter/Return" key when done. The 'Tab' key will move the cursor between fields, or the mouse may be used to position the cursor, which will default initially to the 'Badge #' entry box. The badge number and user ID will be displayed as typed; however, the password characters will only be displayed as asterisks. Once 'OK' or 'Enter' has been pressed, a validity check will be performed to determine that a) both fields contain data and that b) the entered data is of the correct format (as defined in Entrust API). If any field is invalid, the user will be prompted to re-enter them.

If all fields are valid, then the entered User ID, old and new passwords will be submitted to Entrust (external interface) for a password update. If the password change is successful, then control will pass back to step 2.2.2.2.a. The new credentials will be passed to the Upload Credentials function (2.2.2.4.1). If the password change is unsuccessful, then the user will be prompted to reenter the information and the password change will be resubmitted. Three tries will be permitted. After three unsuccessful attempts, the user will be notified that his password has not been changed. The badge activation process will then continue using the old password.

2.2.2.5.2 Entrust Initiated Password Change

The possibility exists that at the beginning of a shift, as the user is performing the authentication and activation sequence, that upon successful entry of the User ID and Password, that Entrust will notify that a forced password change is required. If so, the A&A application should pause its sequence of processing (step 2.2.2.2.a) to perform the following steps.

A change password dialog box will be presented, prompting the user to enter the NEW password twice (once for confirmation), as shown below.

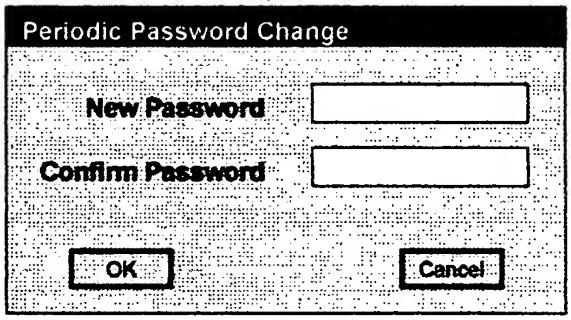


Figure 17. Periodic Password Change Window

The password rules shown in 2.2.2.5.1, above, will be displayed to the user. The user will enter data into both fields, then press 'OK' or the "Enter/Return" key when done. The 'Tab' key will move the cursor between fields, or the mouse may be used to position the cursor, which will default initially to the first password entry box. Password characters will only be displayed as asterisks. Once 'OK' or 'Enter' has been pressed, a validity check will be performed to determine that a) the new and confirm passwords match, b) both fields contain data, and c) the entered data is of the correct format (as defined by the Entrust API). If either field is invalid, the user will be prompted to re-enter them.

If all fields are valid, then the new password will be submitted to Entrust (external interface) for a password update. If the password change is successful, then the process will resume at step 2.2.2.2.a, with the new credentials replacing the old for subsequent badge upload. If the password change is unsuccessful, then the user will be prompted to reenter the information and the password change will be resubmitted.

Three tries will be permitted. After three unsuccessful attempts, the user will be notified that the password change has been unsuccessful and that he should contact the system administrator. The application will return to the main screen.

2.2.2.5.3 [Item Intentionally Deleted]

Section 2.2.2.5.3 was intentionally deleted.

2.2.2.5.4 Password Change at CIS Login

Due to shift boundaries and password timers, the possibility exists that after successfully activating a badge, the user's password may expire and forced to be changed sometime later in the shift, when attempting to log on to the CIS workstation. This situation is addressed in 2.2.3.5.

2.2.2.6 A&A Utilities

In addition to the badge activation functions described above, other administrative utility functions must also be provided as described below. These are accessible from the A&A option window (see Figure 14) and includes:

- Deactivate badge
- Exit application

2.2.2.6.1 Deactivate Badge

For various reasons, the user may need to deactivate a previously activated badge prior to its programmed time-to-live. To do this, the user will initiate the 'deactivate badge' function on the A&A workstation.

Once initiated, this function will prompt the user to enter the logical badge number of the badge to be deactivated. The application will then query the status of this badge using the Badge Technology interface. The application will also query the assignment status of the badge from the authentication database.

Once pertinent badge data has been assembled, the application will make the following checks:

Badge presence. Is the badge to be deactivated currently present?
Badge activation status. Is the badge status showing that the badge is currently active, with an unexpired time-to-live?
Badge assignment status. Is the badge shown as currently assigned?

If the badge is present, then the serial number reported by the badge will be compared against the badge serial number obtained from the database. If these match, processing will continue. If they do not match, the user will be asked to reenter the logical badge number up to three times. If no match occurs by this time, the user will be notified and the application will return to the main screen.

If the badge is present, active, and the serial numbers match, the title and name for the assigned User ID will be retrieved and a message displayed to the user as follows:

"Hello Dr. Jones. Are you sure you want to deactivate Badge number XX?"

'Yes' and 'No' options will be provided. If 'No' is selected, the application will return to the main screen. If 'Yes' is selected, the application will write to the badge as follows:

- Badge will be reset.
- Badge activation will be set to false.
- All user data on the badge will be erased.

Then, the badge activation status in the authentication database will be changed to DEACTIVATED. The user will then be notified that the badge has been deactivated and that the badge should be returned to the badge return area or the system administrator.

If the badge is not present, the user will be prompted to position the badge for writing, and the badge query will be retried. After a preset timeout period (see INI file), the user will be prompted that the badge deactivation failed and to return it to the administrator. If upon repositioning, badge presence is detected, then deactivation will continue as described above.

If the badge is present, but inactive, the application will notify the user that the badge is already deactivated. The application will then return to the main screen.

2.2.2.6.2 Exit Application

Upon selecting "Exit Application" from the A&A Options window, a dialog box will be displayed asking "Are you sure you want to exit?" 'Yes' and 'No' options will be provided. If 'No' is selected, the application will return to the options menu. If 'Yes' is selected, the application will be gracefully shut down.

2.2.3 Application Login (Extension)

Application login verifies the identity of users and grants or denies them access to the CIS Client application at a given workstation. It runs on each BARB equipped CIS workstation. Login occurs using the wireless token, but does not preclude manual login to the CIS Client application via entry of User ID and password.

This function is composed of the following subfunctions, which are described in the following subparagraphs.

- Maintain login state
- Get badge info
- Query badge status
- Proxy credentials
- Password update

The functional flow diagram for the application login function is shown below in Figure 18.

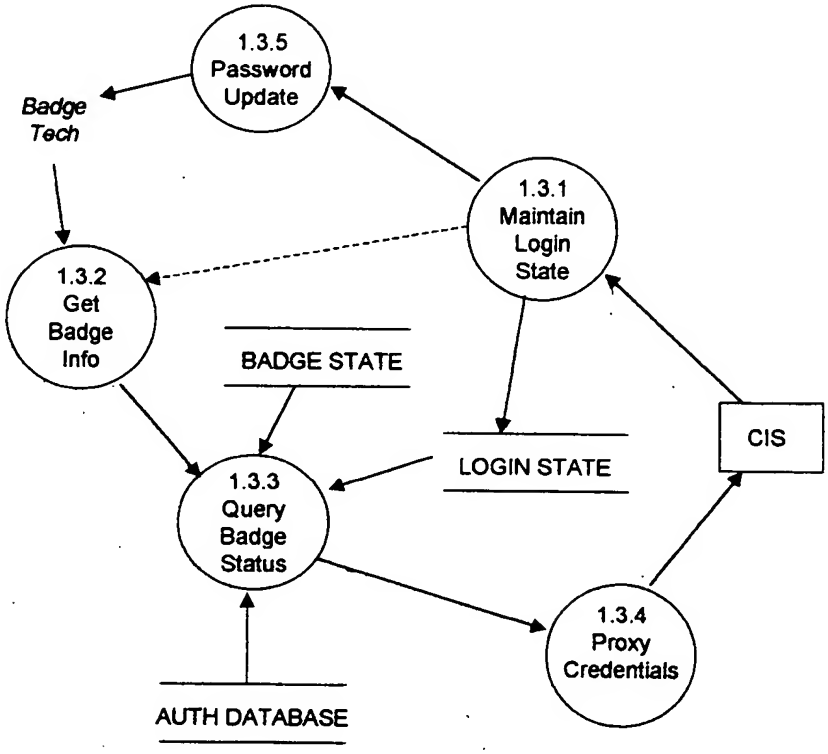


Figure 18. Data Flow Diagram for Login Application

2.2.3.1 Maintain Login State

The CIS Client will notify the Login enhancement when the CIS login screen is up (displayed and ready to accept inputs). This function will maintain a dynamic state table, which will keep track of the state of the login process. Possible states are:

- Ready for login ("ready state")
- User currently logged on ("busy state")
- Wait state

The system is considered ready for login following such notification from the CIS Client. At this point, badge login is enabled. If a badge is recognized during this state, a badge login will be attempted.

A user is considered to be logged on when the CIS Client notifies the login enhancement of a positive login result, whether that login was initiated by the login enhancement or was accomplished manually. This state is analogous to a "busy" state. While any user is logged on to the CIS Client, no other user may be logged on to the same CIS client, regardless of badge detection. This function will maintain in a table the currently logged on user, by User ID.

The system is considered to be in a "wait" state under the following conditions:

- A syntax check has been received, but no login result or 'logon screen up' notification has yet been received.
- A negative login result has been received, but no 'logon screen up' notification has yet been received.
- A 'logoff/lockup' notification has been received, but no 'logon screen up' notification has yet been received.

- A badge login has been sent to CIS, but results have not yet been returned.
- A CIS shutdown notice has been received, but the login application has not yet shutdown.

When the system is in the 'wait' state, no badge logins may be attempted. However, the login application must track the badges that become present during the wait state, and the order in which they appeared so that the first appearing badge still present may be logged on once the state changes to ready for login. This represents the login candidate list.

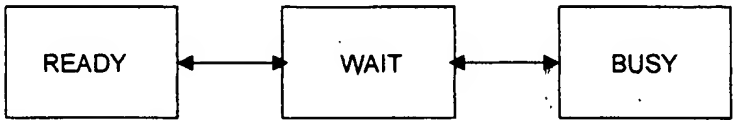


Figure 19. Login State Transition

This function also maintains a table as to recently logged off users (by User ID/badge number). Once logged off, a delay period is initiated during which time that user may not be logged back in. [This is to avoid inadvertent login immediately following logout, but before the user can leave the room.] Once the delay ("badge cloaking") time has run out, the user is removed from this "no login list" and may be logged in. The badge cloaking delay period is set in the INI file.

A table is kept of recently failed badge logins. After a badge login failure (either due to syntax or credentials) is reported by the Proxy Credentials function, that User ID is added to the "no login list", so that the individual whose badge failed to properly log him in will not be precluded from manually logging in. The user will remain on the "no login list" until he is determined to have left the room (i.e., badge is no longer present). Failed manual logins will not be tracked as these are handled directly by CIS.

The "no login" table is described in Section 4.4.

2.2.3.2 Get Badge Info

When the presence of a badge is recognized, the Badge Technology interface will send a badge state report to the login enhancement as an update to the badge state table. [The Application Login enhancement should always possess a current badge state table.] If the system is in a 'ready for login' state, then the first arriving badge that is a) still present and b) not on the "no login list", will become the login candidate. The Get Badge Info function will then query the login candidate badge for its status and login credentials. In response to this query, the badge interface should return the following information:

- Badge serial number
- Badge status
- User ID
- Password
- Time to live

First, the login enhancement must decrypt the user data (user ID and password) using the encryption key obtained from the key holder (2.2.8.1) during startup. Then, the badge is checked to ensure that it is acceptable for logon purposes. To be acceptable, the badge must meet the following criteria:

Time to live/activation indicator. UNEXPIRED (DTG is later than current time)/ACTIVATED
On person indicator (if enabled). ON PERSON
Probability of removal (if enabled). ≥ Minimum Confidence (set in INI file)
KP ID inserted indicator (if enabled). INSERTED
KP ID removal indicator (if enabled). NEVER REMOVED

If any of the above criteria are not met, then the badge will be added to the 'no login list' until departing the area. The next badge on the login candidate list (if any) will then be selected and this function repeated for that user.

If the above criteria are met, the badge information is then passed to the Query Badge Status function (below).

2.2.3.3 Query Badge Status

Upon receipt of candidate badge data, this function will query the authentication database to determine the status of this badge. If the badge is found to be valid (badge assignment status = assigned and badge activation = activated), then the user's credentials (User ID and Password) will be passed to the Proxy Credentials function (below).

If the badge is found to be invalid, then it will be added to the 'no login list' until departing the area. The next badge on the login candidate list (if any) will then be selected and the 'Get Badge Info' function will be invoked.

2.2.3.4 Proxy Credentials

Upon validation of the badge and receipt of credentials, this function will interface to the CIS Client to pass these credentials in to initiate a badge login to CIS. This will follow the interface definition for the CIS Client login modifications. Once the login request has been made, this function will notify the Maintain Login State function, so that the state can be changed to 'wait'. The CIS Client will respond with the following returns:

- Syntax check result
- Login result

The syntax check should be positive since it is an automated interface, unless an error in transmission has occurred. If a negative syntax check is received, the badge will be added to the 'no login list'. [This is to avoid the "three times and you're out" feature of CIS and to allow for a manual login.] If the syntax check is positive, the system continues to wait for the login result.

Upon receipt of the login result, if the result is positive, then the login enhancement Maintain Login State function will be notified so that the state may be changed to 'busy' and the logged on User ID can be posted. If a negative result is received, then the Maintain Login State will also be notified, so that the badge can be added to the 'no login list' to allow for a manual enrollment. [This might occur if a password change occurred subsequent to badge activation, so the badge contains old credentials. If so, the 'Password Update' function (below) will be invoked.]

2.2.3.5 Password Update

In the event of a failed automatic badge login, other than for syntax reasons, a possible reason is that a password change occurred subsequent to badge activation. This function attempts to recover from this condition.

If after an attempted automatic badge login, notification is received from CIS of a login failure AND an immediate (time defined in INI file) notification is received from CIS of a successful (manual) login, then:

If User ID for the failed badge login and the successful manual login are the same, AND the Password for the failed badge login and the successful manual login are different, then it is assumed that a password change has occurred and the new (successful manual) password will be written to the badge. [NOTE: This logic is located within the CIS Client login modification.]

To do this, the badge must be detected to be present by checking the badge state table. If the badge is not present, this function will not be performed. If the badge is present, then the new password will be uploaded to the badge as described in Section 2.2.2.4.1 (except that only the password will be written - all other data will remain unchanged).

2.2.4 Biometric Technology

The biometric technology function represents commercial-off-the-shelf (COTS) components comprising the biometric interface, module, and devices. It is accessed by the Authentication Administration function and the Authentication & Activation function. It is composed of the following subfunctions, which are described in the following subparagraphs.

- HA-API interface
- Fingerprint BSP
- Iris BSP

The functional flow diagram for the biometric technology function is shown below in Figure 20.

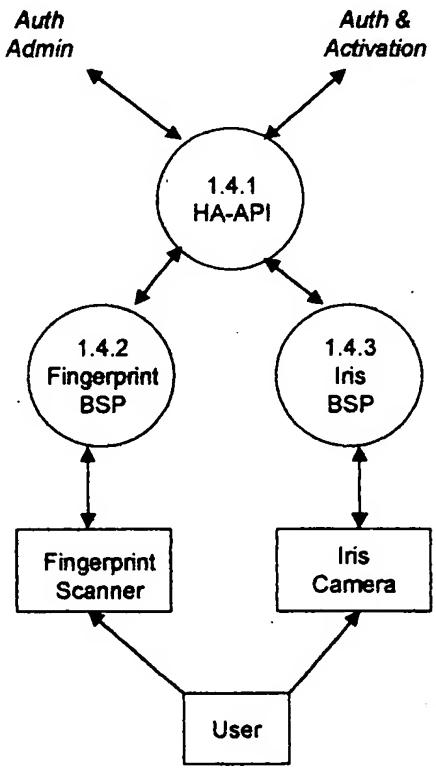


Figure 20. Biometric Technology Data Flow Diagram

2.2.4.1 HA-API Interface

The Human Authentication API (Version 1.03) will be used in the pilot as the standard biometric interface through which the biometric technology is accessed. The HA-API runtime software will be included as a COTS component. This interface is defined in the HA-API Specification. HA-API communicates directly to and manages any HA-API compliant BSPs installed in the system.

2.2.4.2 Fingerprint BSP

A Biometric Service Provider (BSP) module packages the biometric algorithms needed to perform a biometric capture, process, verify, and enrollment. For the pilot, one or more fingerprint BSPs will be installed on the workstation. The BSP interfaces directly with the biometric capture device (in this case, a fingerprint scanner) and the user to perform the requested operation. Any graphical user interface required to perform these operations is performed by the BSP.

2.2.4.3 Iris BSP

The iris BSP also performs the biometric capture, process, verify, and enrollment upon request. It interfaces directly to the iris scanning camera, which is the biometric capture device, and to the user. Any graphical user interface required to perform these operations is performed by the BSP.

2.2.5 Badge Technology

The badge technology function represents components comprising the wireless badge interface, module, and devices. The badge technology may be an existing COTS product (e.g. RF Ideas) or a new design not yet commercially available. It is accessed by the Authentication & Activation function and the Login Application function. It is composed of the following subfunctions, which are described in the following subparagraphs.

- Application interface
- Enumerate badges
- Read badges
- Write to badges
- Maintain badge state
- Receive event
- Poll badges
- Badge #1 SDK (RF Ideas)
- Badge #2 SDK (To be determined)

The functional flow diagram for the badge technology function is shown below in Figure 21.

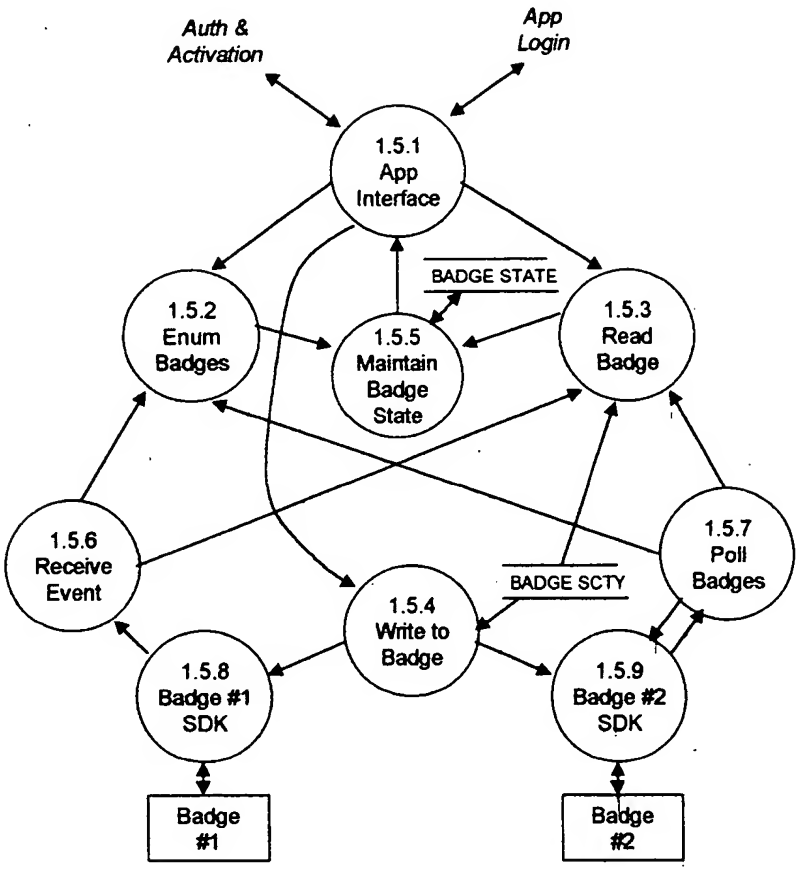


Figure 21. Badge Technology Data Flow Diagram

2.2.5.1 Application Interface

This function provides a standard interface for the application to interface to a wireless token. Since two such tokens are envisioned to be supported for the pilot, the interface to the application is designed to be the same in both cases. The following badge functions are expected to be available for the application:

Function	Information passed in	Information returned
Initialize interface	Callback data	Badge state table (all badges)
[Callback]	[Receiver]	Event data
Enumerate badges	Request	Badge state table (all badges)
Ping badge	Badge serial number	Success or failure
Request badge status	Badge serial number	Badge status (specific badge)
Reset badge	Badge serial number	Success or failure
Initialize badge	Badge serial number, global password,	Success or failure
Write badge data	Badge serial number, User ID,	Success or failure

	password, (with tags and password)	
Delete badge data	Badge serial number, tag/password or global password (delete all)	Success or failure
Read badge data	Badge serial number, tag, password	Badge data (User ID, password, time-to-live)
Activate data pre-read	Data tags	Success or failure
Request expiration time	Badge serial number, global password	Expiration DTG
Activate badge	Badge serial number, time-to-live, global password	Success or failure
Get/Set badge parameters	Badge power (badge serial #) Base sensitivity Visible timeout Lost Badge timeout	Badge power Base sensitivity Visible timeout Lost Badge timeout
Get/Set on-badge features	Badge serial number – Indicator status Playtone Playwave Clock Date	Indicator status Clock Date

The application interface will use the callback to send the badge state table whenever a change to this table occurs, either due to the arrival/departure of a badge or change in status of a badge.

NOTE: The badge time-to-live is set at the time the badge is activated, as opposed to as an explicit data write operation.

2.2.5.2 Enumerate Badges

This function is used to determine what badges are present in the vicinity of the workstation. A list of badges, by badge number are returned to the application as a result of this function, in descending order of appearance time (first appearing to last appearing). This data will be received from the badge SDKs in three ways depending upon badge architecture: (a) badge is polled by badge service provider for this information (used by RF Ideas badge), (b) badge may automatically beacon its presence, or (c) badge base station may provide polling functionality in firmware/hardware..

This function also sends badge information to the Maintain Badge Status function (see 2.2.5.2) to maintain a state table of all badges present and retrieves current state when needed.

In determining continuous badge presence, a "flicker factor" is to be implemented. This is intended to eliminate brief periods where badge presence cannot be detected but the user is still in the immediate vicinity (for example, when the user moves behind an obstruction, turns away, or bends down out of view of the transceiver). Therefore, a default filter delay time is set (check INI file for value). If the period of non-detection is below this delay time, the user is still considered present and his lack of detection during that period is not reported to the application. If the period of non-detection exceeds the flicker time delay, then the user is considered to have left the vicinity and is removed from the state table. If the user then reappears, he is re-added to the bottom of the state table. Thus, a delay timer must be set/reset for each user depending on consecutive detection intervals. The default flicker factor is 3 seconds.

2.2.5.3 Read Badge

When requested by the application, this function queries the badge to return data stored on-board the badge. Badge data is stored in the following format:

Data tag. The identifying tag number associated with the specific data element.
Data. The stored data element content.
Data password. The password required to access the stored data element.

Data to be stored on the badge includes the following:

Data Tag	Data Element	Description	Format
UID	CIS/Entrust User ID	User ID of the user to which the badge has been assigned as a result of a successful activation.	Annnnnn
UPW	CIS/Entrust User Password	Password of the user to which the badge has been assigned as a result of a successful activation.	8 - 16 alphanumeric characters

In order to read the data from the badge, the following is needed:

- Decryption key
- Data password(s)

All data is password protected and encrypted (prior to being written). In order to access and read this data, this function must provide a valid password (i.e., one which matches the stored data element password). The data will be decrypted by the application. Once these steps have been performed, the data is ready to be provided to the requesting application.

For the pilot, a single data password will be used and will be hard-coded into the application.

2.2.5.3.1 Data Pre-Read

The badge interface may perform a data 'Pre-Read', when activated. This allows data elements to be read off the badge and cached in anticipation of a request from the application. Upon determination that a new badge is present, the badge interface performs a read of the two data fields listed above. These are held until a request for this information is received from the application, at which time the data is forwarded to the application without the need to further query the badge. In addition to the cached data, the time cached should also be stored. The badge interface must insure that:

- Pre-read data stored in memory is updated if any of the pre-read fields are updated.on the badge (i.e. data rewritten by the interface). This should only occur on a "password update attempt".
- Pre-read data is not released if the "Expiration" time is reached.

2.2.5.4 Write To Badges

When requested by the application, this function writes data to the storage area of the badge. The data written is the same as that described above for the 'Read Badge' function. In order to perform the write, the badge must be present. Data will have been previously encrypted by the application. This function must store the data with the proper tags and passwords.

2.2.5.5 Maintain Badge State

This function maintains a badge state table as to what badges are present at a given point in time and what their current status is. Information maintained in the state table consists of the following (for each badge present):

Badge serial number: manufacturers serial number of badge
Badge status: specific status bits (see below)
Time first appearing: time the badge presence first detected (this session)
Time most recently seen: most recent presence detection (this session)

Badge status will consist of the following data:

Reset status - 1 bit: true or false
Initialized - 1 bit: true or false
Badge on person - 1 bit: true or false
Badge removal confidence - 3 bits (high value = high confidence that badge has been removed)
Activation indicator - 1 bit: activated = true; not activated = false
KPID card inserted - 1 bit: inserted = true; not inserted = false
KPID card removed since activation - 1 bit: removed at least once = true; never removed = false
Battery low indicator - 1 bit: low = 1 (battery charge <4); OK = 0
Battery charge level - 3 bits (0 = discharged; 7 = fully charged)
Time to live indicator - 1 bit: expired = true; not expired = 0

Note that the table will be ordered from first appearing badge to last appearing. It will be updated whenever any new information becomes available. In particular, new badges appearing are added to the bottom of the state table, along with their time of appearance and current status; old badges detected to have left the area (no longer present, after flicker delay) are removed from the list; and existing badges with continuing presence will be updated as to most recent time seen and any changes in status bits.

The badge state table will be passed to other functions or the application upon request.

2.2.5.6 Receive Event

For badges which broadcast their presence, this function will act as the receiver of that event. Events are received from the badge SDK. It will pass pertinent data along to other functions, which maintain state or interface with the application to notify it of significant events (such as the Enumerate Badges function).

2.2.5.7 Poll Badges

For badges which do not broadcast their presence (such as the design by RF Ideas), this function will periodically poll the badges to determine their presence, via the badge SDK. For the pilot, since a small number of badges will be in use, the polling will be done by circulating through a list of badge serial numbers. The list of badge serial numbers will be read from the INI file during start-up. The polling will be continuous, with a single cycle time depending on the response time of the badge technology. The polling interval will be set in the INI file. During the polling, as badges are determined to be present or not present, this information is passed back to other functions which maintain state or interface with the application to notify it of significant events (such as the Enumerate Badges function).

2.2.5.8 Badge #1 (RF Ideas) SDK

The RF Ideas' badge SDK is a COTS product provided by the badge manufacturer as a means of interfacing to the particular badge technology. The badge interface must conform to the SDK API and use the available functions and capabilities to perform the functions described in the Badge Technology functions, above.

The badge utilizes RF communication with the following features and capabilities:

- Polling interface
- Limited on-board memory
- No ability to detect removal from body
- No ability to detect insertion of KP ID badge

This badge will be implemented for probable BARB project deployment.. Note that the pilot system must work with either badge #1 or #2, and that the same interface must be presented to the application, regardless of badge technology implemented. Badge #1's SDK also creates and makes entries into its own local log file.

The Badge SDK will be implemented within an NT service.

2.2.5.9 Badge #2 SDK

Kaiser has not yet committed to a vendor for Badge #2. It is anticipated that the badge will incorporate some, or all, of the following features and capabilities:

- Broadcast presence or intelligent polling base station
- Significant on-board memory and processing power
- On-board encryption supporting encrypted communication with the host (encryption capability may be incorporated in a vendor supplied base station or may be provided in software running on the workstation).
- On-board sensors and indicators (visible and/or audible)
- On-board clock
- Support a timeout functionality (e.g. Time-to-Live)
- Ability to detect presence on a body (instantaneous measurement)
- Ability to detect removal from the user's body
- Ability to detect insertion of KP ID badge (instantaneous measurement)
- Ability to determine that the KP ID badge had been removed.
- Ability to self-deactivate (e.g. due to removal, due to expired Time-to-Live, etc.).

2.2.6 Biometric Server

The biometric server is a COTS product whose specifications are delineated in commercial documentation.

Note: Information provided about the SAFServer is limited due to data rights and IP issues. Any information provided herein regarding this server is proprietary to SAFLINK Corporation and is excluded from the data rights clauses of the contract.

The biometric server application will perform the following functions:

- Performing additions and deletions of user records from the biometric enrollment database
- Biometric verifications to determine if a captured biometric sample matches the previously enrolled sample for the claimed identity

Figure 22 is the data flow diagram for the biometric server function.

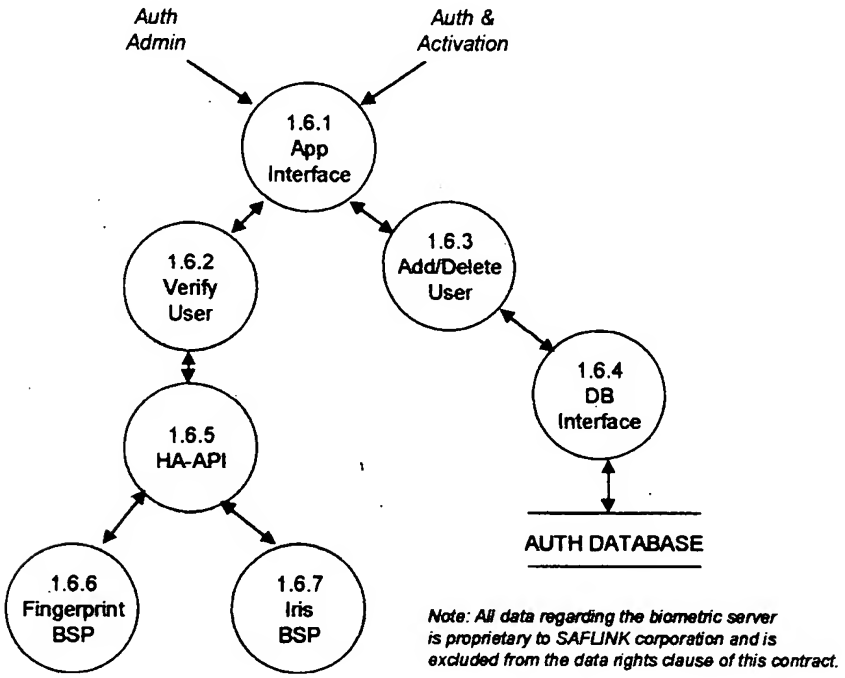


Figure 22. Biometric Server Data Flow Diagram

The biometric server interfaces to the Authentication Administration function to perform biometric enrollments and maintenance of the user biometric records and to the Authentication & Activation application to perform biometric authentications. It also interfaces to the authentication database for storage and retrieval of user biometric data. It conforms to the HA-API in order to interface to the installed biometric technologies, which perform the actual matching operations. The HA-API and BSP functions are the same as those described in section 2.2.4.

Note that in order for a biometric verification to occur, the following must be true:

- The user must be enrolled in the biometric technology to be verified.
- The biometric technology used to perform the biometric capture and processing at the workstation must also be installed on the biometric server (less capture device).

Biometric data stored within the authentication database by the Biometric Server will be encrypted prior to transmission and storage using RSA RC4 128-bit encryption. Also, communication with the client applications will be encrypted using RSA RC4 128-bit encryption with session keys, using Diffie-Hellman key exchange.

The biometric server and authentication database are planned to execute on the same NT platform, which will be replicated for redundancy/failover purposes (see 5.0, Security and Availability).

2.2.7 Auditing

The auditing function will execute as a separate DLL on the local workstation hosting one or more of the three main applications, with local text files being generated. It will collect audit event information from all of the other system functions and post it to an audit log file. It is composed of the following subfunctions, which are described in the following subparagraphs.

- Create audit log
- Receive audit record
- Post audit record
- Sort audit log [future]
- Archive audit log [future]
- Print audit log [future]
- Clear audit log [future]

The functional flow diagram for the audit function is shown below in Figure 23.

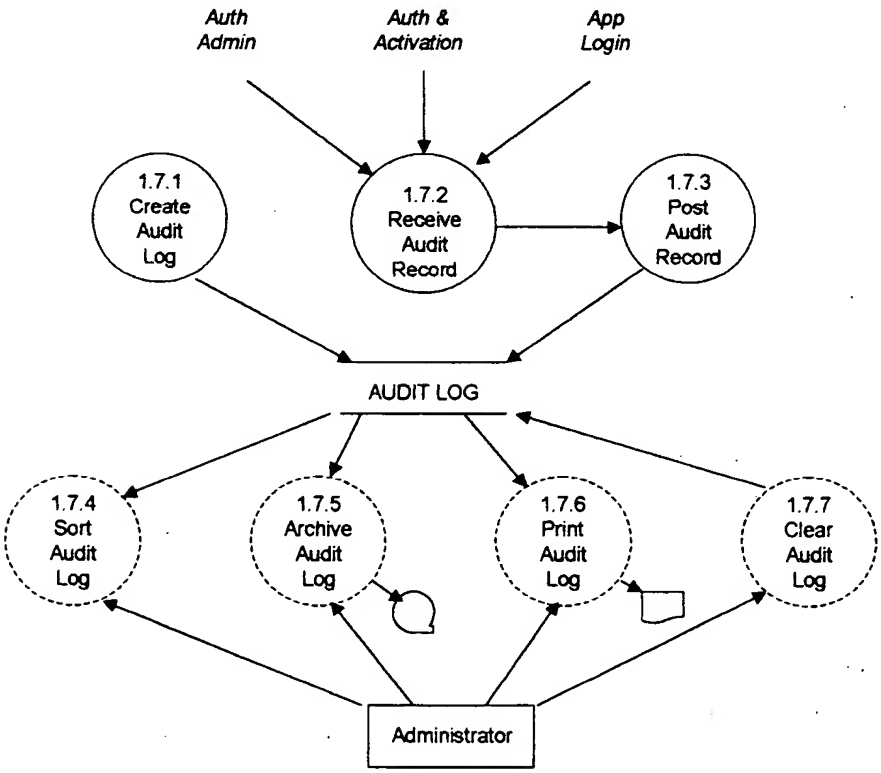


Figure 23. Audit Function Data Flow Diagram

2.2.7.1 Create Audit Log

Upon activation of the audit function, a check will be made to determine if the audit log (text file) exists. [This file will be named BARB.log and located within the BARB director.] If the file exists, then this function does nothing. If the file does not exist, it is created by this function. The first entry into the audit log will be the creation event.

2.2.7.2 Receive Audit Record

When one of the system applications creates an entry for the audit log, it is packaged and sent to the auditing function. The package may contain one or more audit records. All audit records will contain the following information:

- Date/time of event
- Event tag
- User ID (or N/A)
- Workstation ID (host name)
- Badge Serial Number (or N/A)
- Badge status bytes
- Posting application ID
- Event data

Application IDs are assigned as follows:

Application	ID
Authentication Administration	ADM
Authentication & Activation	A&A
Application Login Enhancement	ALE
Badge Interface	BIF

Events to be audited include the following, as a minimum:

Event tag	Event	Event Data
000	Audit log creation	
A01	Administrator logon to Authentication Administration application	Admin ID
A02	User created	User ID
A03	User deleted	User ID
A04	User edited	User ID
A05	Badge created	Badge ID
A06	Badge removed from service	Badge ID
A07	Badge revoked	Badge ID
A08	Badge reinstated	Badge ID
A09	Badge turned in	Badge ID
A10	User biometric enrollment	User ID, BUID of enrollment technology
A11	Change in biometric preference	User ID
B01	Badge activation initiated	User ID, Badge ID
B02	Badge activation successful	User ID, Badge ID, TTL
B03	Badge activation unsuccessful	User ID, Badge ID 01 - Failed badge presence 02 - Badge number mismatch 03 - Badge # does not exist 04 - Badge already assigned 05 - Badge invalid 06 - Low battery

		07 - Badge not on person 08 - KPID not inserted 09 - User does not exist 10 - User already has active badge 11 - Exceeded max # unreturned badges 12 - Failed credential check (password no-match) 13 - No biometrics enrolled 14 - Biom tech not installed 15 - Failed biometric auth (no-match) 16 - Failed badge write 17 - User cancelled activation
B04	Password change – successful	User ID Change type: 01 = User initiated 02 = System initiated
B05	Password change – unsuccessful	User ID Change type: 01 = User initiataed 02 = System initiated Failure reason: 01 - Old password invalid 02 - New password unacceptable 03 - User cancellation
B06	Badge deactivation by user	User ID, Badge ID
B07	Biometric capture	User ID, BUID, Biometric Type
C01	Badge login successful	User ID, Badge ID
C02	Badge login - unsuccessful	User ID, Badge ID 01 - syntax error 02 - credential error
C03	User logoff	User ID, Badge ID
C04	Badge state table update	New state table
C05	Password update	User ID, Badge ID Results: 1 = successful 0 = unsuccessful
T01	Biometric technology failure	BUID, Error code
T02	Badge technology failure	Badge type, Error code
T03	Biometric server failure	Error code (if available)
T04	Network failure	

2.2.7.3 Post Audit Record

Audit records will be posted to a local disk file. The audit log will be 140 byte; tab delimited text file, suitable for import into a spreadsheet or database. All event data (other than User ID and Badge ID, which have their own fields) will be tagged and/or coded.

As records are received, they are appended to the existing audit file.

See Section 4.3 for audit file description.

2.2.7.4 ARM Log

In addition to the customized audit log capability described above, the A&A application will also post specific (relatively high level, user related) transaction type events to the Tivoli system ARM log. All ARM postings will also be recorded in the Authentication Audit log. ARM events to be recorded include the following:

Activate session:

- Database query to check badge availability
- Validate and initialize badge
- Check entrust credentials
- Biometric Authentication – Fingerprint
- Biometric Authentication – Iris
- Upload and activate badge
- Database update – badge activation/assignment status

Deactivate session

- Database query to check badge availability
- Initialize badge
- Database update – badge status

Password Change session:

- Entrust credential check
- Entrust password change

For each of the above events, start and stop transactions will be logged. A separate transaction will be reported for each biometric authentication attempt.

2.2.7.5 Future Capabilities

For the pilot, existing platform utilities will be used to handle the created and populated text audit file. In the future, a more sophisticated auditing capability and format is expected to be developed, to include security features such as access control, confidentiality, and integrity protections. In addition, additional functions are expected to be developed to perform the following:

- Sort Audit Log
- Archive Audit Log
- Print Audit Log
- Clear Audit Log

Also, in the future, a central server-based audit capability is planned.

2.2.8 Ancillary functions

In addition to the main functions/applications described above, there are a couple of additional ancillary functions that must also be implemented. These include:

- Badge encryption key management
- Badge parameter adjustment

2.2.8.1 Badge Encryption Key Management

As described previously, all data written to the badge must be encrypted prior to writing to the badge (and decrypted after reading from the badge). They key used to perform this must be generated, stored, and disseminated centrally, so that a badge written at one workstation may be read at another.

A Badge Key Management utility application will be provided to perform the badge key management function. This application will run on the biometric server platform and utilize the authentication database as the storage location. Upon initialization, the A&A and Login Extension applications will retrieve the current key from the repository.

2.2.8.1.1 Key Generation

The Key Manager will randomly generate 128-bit keys using the facilities of the CryptoAPI available on the Windows NT platform. RSA RC4 symmetric keys will be used. The key itself will be encrypted prior to storage. Protection of this key will be via the same mechanism as used by the biometric server for the biometric data.

2.2.8.1.2 Key Storage

Keys will be stored in encrypted form within the authentication database. Password access control will also be in place. The key will also be written to a floppy disk for key escrow purposes. A method of reading in the key from the floppy to replace a corrupted or compromised key will be provided.

2.2.8.1.3 Key Dissemination

Keys will only be disseminated to authorized applications based on a shared secret. Keys will be disseminated via secure channels only.

2.2.8.2 Badge Parameter Adjustment

Through the badge SDK API, the properties of the badge transceiver (also known as a base station) can be adjusted to the configuration and unique characteristics of the room/environment in which it is installed.

A capability will be provided to allow these properties to be "manually" adjusted at a given workstation location. Properties to be adjusted include the following (note: by definition, these settings are technology dependent):

-
- Base station sensitivity (RFID, possibly 2nd badge technology)
- Badge transmit power (possibly 2nd badge technology)
- Visibility timeout
- Lost badge timeout
-

Default values for these parameters will exist in an INI file (settings will be technology dependent). Adjusted values will overwrite the defaults. See section 4.4 for file description.

Parameters which will only be stored and accessed via the INI file include the following:

Flicker filter delay timeouts
Badge maximum delay
Badge polling interval (RFID only)
Retransmission retry counter (RFID only)
Base station receiver attenuation

2.2.9 Database Server

The database server provides a common interface from the various applications (2.2.1 – 2.2.3) to the BARB database for secure access to user and badge information. The biometric server (2.2.6) provides access to the biometric portion of the database. The database server is located on the same platform as the biometric server and shares a common database.

Communication from the applications to the database server will be encrypted using RSA RC4 128-bit encryption with session keys, using Diffie-Hellman key exchange. Sensitive data (i.e., administrator passwords) will be encrypted when stored using RSA RC4 128-bit encryption.

The database server and authentication database are planned to execute on the same NT platform, which will be replicated for redundancy/failover purposes (see 5.0, Security and Availability).

3.0 Process Flows

This section provides a high level depiction of the operational process flows within the three primary functional areas or applications:

- Authentication Administration
- Authentication and Activation
- Application Login

These operational sequence diagrams are not intended to convey a detailed design or use case scenario, but to depict the general process flow. To read the diagrams; the columns depict system components. Events, activities, or processes are shown within rectangular boxes. Decisions are shown as diamonds. Data or control flows are shown as arrows. The sequence in time is read downwards from top to bottom.

Note that the processes described to not typically include exception processing.

3.1 Authentication Administration Process

This section describes the sequence of operational process flows that occur within the Authentication Administration application. Figure 24 shows the process flow.

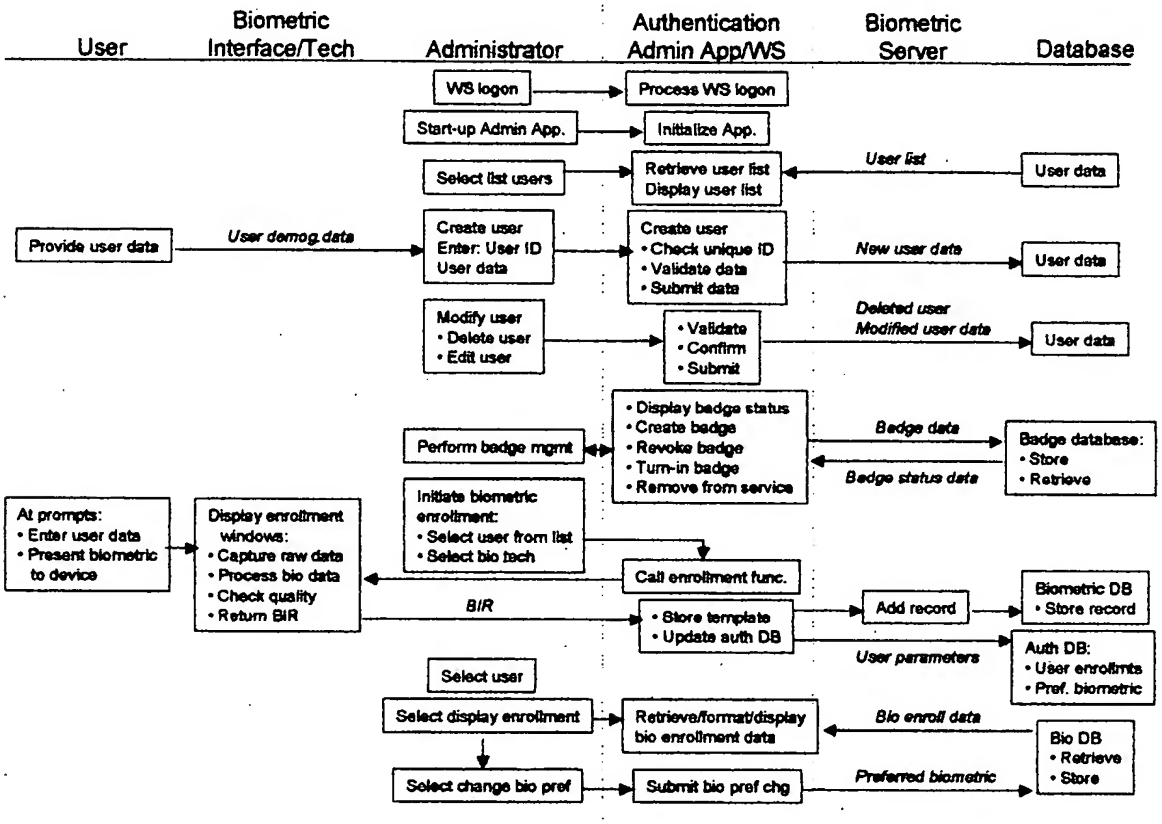


Figure 24. Authentication Administration Process

3.2 Authentication and Activation Process

This section describes the sequence of operational process flows that occur within the Authentication and Activation application. Figure 25 shows the operational sequence diagram for the Authentication and Activation application.

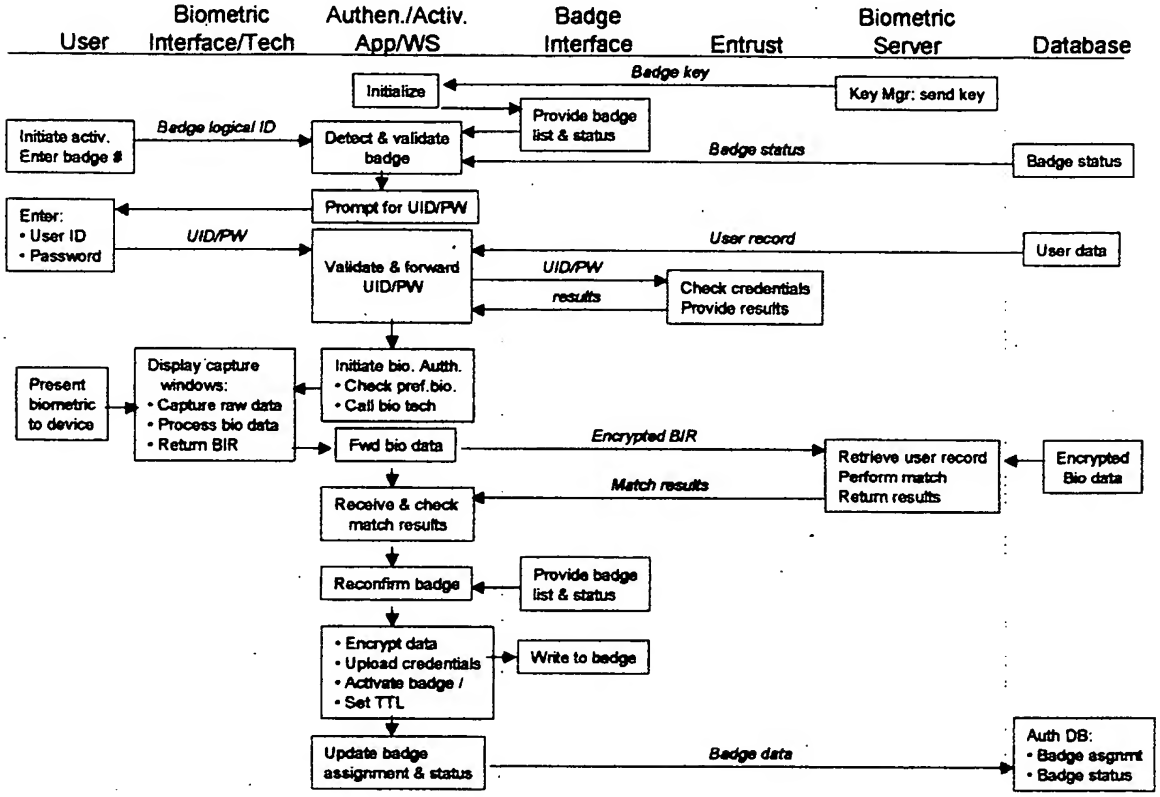


Figure 25. Authentication & Activation Process

3.3 Application Login Process

This section describes the sequence of operational process flows that occur within the Application Login function. Figure 26 shows the operational sequence diagram for this function.

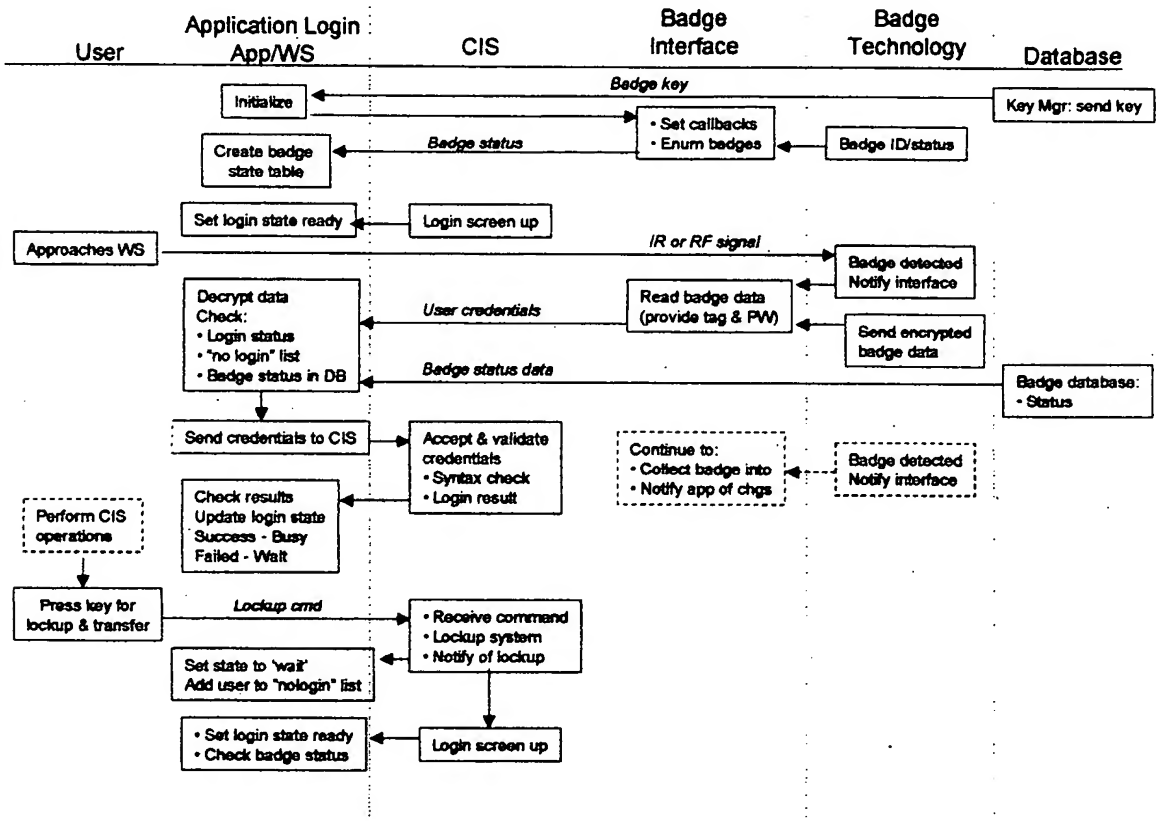


Figure 26. Application Login Process

4.0 Data Elements

This section defines the stored data elements for the enhanced CIS authentication system.

4.1 Authentication Database

4.1.1 User Data

User data is contained in the following tables:

USER MAIN

Field Name	Field Size	Field Type	Description
User ID	7 B	String	A unique string value consisting of a beginning alpha character followed by 6 numeric characters.
Last Name	35 B	String	User's family name.
First Name	25 B	String	User's given name.
Middle Initial	1 B	Char	User's middle initial. Blank if none.
Title	6 B	String	User's title (Dr., Mr., Mrs., etc.). Not job position.
Department	30 B	String	Name or number of user's assigned department.
Phone Number	15 B	String	User's office phone number (numeric). Includes 3 digit area code, 7 digit phone number, and optional extension (up to 5 digits).
Tie Line	3 B	String	User's tie line prefix.
Email Address	48 B	String	User's KP email address.
Default Badge Time-to-live.	4 B	Integer	Number of hours for which the user's badge will be activated, before expiration. Default = 12 hours.

USER BIOMETRIC PREFERRENCE *

Field Name	Field Size	Field Type	Description
User ID	7 B	String	A unique string value consisting of a beginning alpha character followed by 6 numeric characters.

Biometric Preference	128-bit	Binary/Hex	BUID of preferred biometric technology.
Account password	16 B	Binary	Not used.

BUID = Biometric Unique Identifier (HA-API definition)

* Tables indicated with an asterisk are standard SAFserver tables, which will be utilized unmodified.

4.1.2 Administrator Data

ADMINISTRATOR MAIN

Field Name	Field Size	Field Type	Description
User ID	7 B	String	A unique string value consisting of a beginning alpha character followed by 6 numeric characters.
Last Name	35 B	String	User's family name.
First Name	25 B	String	User's given name.
Middle Initial	1 B	Char	User's middle initial. Blank if none.
Title	6 B	String	User's title.
Department	30 B	String	Name or number of user's assigned department.
Phone Number	15 B	String	User's office phone number (numeric)
Tie Line	3 B	String	User's tie line prefix.
Email Address	48 B	String	User's KP email address.
Password	16 B	Binary (encrypted)	Administrator's backup password for access to the Auth Admin application.

4.1.3 Badge Data

BADGE INVENTORY

Field Name	Field Size	Field Type	Description
Badge Serial Number	4 B	Ulong	A unique number assigned by the badge manufacturer (in badge ROM and visually readable on badge surface).
Badge Logical ID	1 B	Integer	Badge number assigned by administrator. [May also be affixed to badge.
Badge Type	4 B	String	Type of badge technology (RFID or HPIR).

BADGE INVENTORY STATUS

Field Name	Field Size	Field Type	Description
Badge Serial Number	4 B	Ulong	The manufacturer's serial number of the badge.

Badge Assignment Status	1 B	Char	1 = "assigned" 2 = "available" 3 = "out of service"
Badge Activation Status	1B	Char	1 = "activated" 2 = "deactivated" 3 = "revoked" 4 = "inactive"
User ID Assigned	7 B	String	A unique string value consisting of a beginning alpha character followed by 6 numeric characters.
Date/time of activation.	8 B	Datetime	Date and time of most recent activation (GMT).
Date/time of expiration	8 B	Datetime	Date and time of expiration for most recent activation (GMT).
Last turn-in time	8 B	Datetime	Date and time that badge was most recently returned. (GMT)
Comment	79B	String	Badge annotation, particularly why a badge was removed from service.

Notes -

(1) Datetime format displays as: dd/mm/yyyy hh:mm:ss XM.
(2) Time displayed at workstations as local time.
(3) Time stored within and displayed at server (via DBMS viewer) as GMT.

4.1.4 Biometric Data

BIOMETRIC DATA (multiple) *

Field Name	Field Size	Field Type	Description
User ID	7 B	String	A unique string value consisting of a beginning alpha character followed by 6 numeric characters.
Biometric Technology ID	4 B	Integer	BUID of creating BSP
BIR	Variable	Binary	Biometric Identifier Record containing the enrolled biometric template(s) created by the enrolling BSP.
Raw BIR	Variable	Binary	Not used.

BIOMETRIC TYPE CROSS-REFERENCE (multiple)

Field Name	Field Size	Field Type	Description
Biometric Technology ID	4 B	Integer	BUID of BSP
Biometric Type	2B	Mask	Type of biometric technology (i.e., fingerprint, face, voice, iris ...) [Use as defined in BioAPI]

4.1.5 Authentication Database Schema

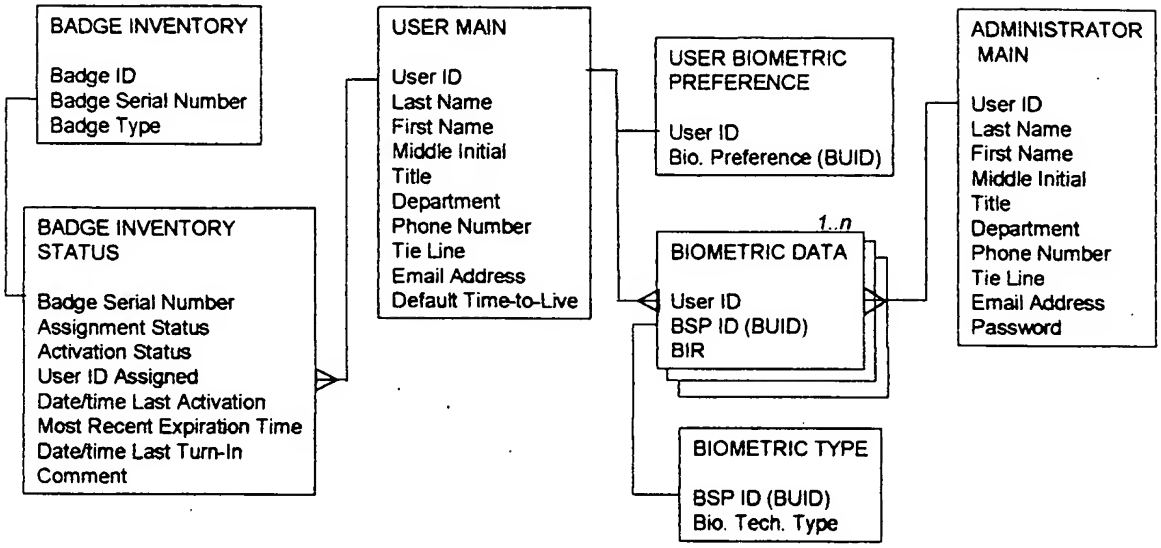


Figure 27. Authentication Database Schema

4.2 On-Badge Data

Data stored on the badge is as follows:

TAG	DATA	PASSWORD

Data Tag (ulong)	Data Element	Description	Format
UID	CIS/Entrust User ID	User ID of the user to which the badge has been assigned as a result of a successful activation.	annnnnn
UPW	CIS/Entrust User Password	Password of the user to which the badge has been assigned as a result of a successful activation.	8 - 16 alphanumeric characters
TTL	Time-to-Live/Expiration date/time	Time at which the badge will become expired/inactive.	DTG

Note: TTL is not stored as user data in Badge #2, but is set as an expiration timer.

For the RFIDeas badge, the 2 16-bit registers will be populated as follows:

Register 1: UUUUUUU SSSSDDDD
0123456701234567
Register 2: PPPPPPPPPPPPPPPP

Where:

UUUUUUU	User ID
SSSS	Status Bytes

DDDD	Time to Live (date/time)
PPPPPPPPPPPPPPP	Password

4.3 Audit Log

Field Name	Field Size	Field Type	Description
Event Tag	3 B	String	Tag identifying type of event (see Sec 2.2.7.2 for tag assignments)
Date/time of Event	14 B	String	Date and time the event occurred (YYYYMMDDHHMMSS)
User ID	7 B	String	A unique string value consisting of a beginning alpha character followed by 6 numeric characters.
Workstation ID	32 B	String	Host name of workstation where event occurred
Badge Serial Number	10 B	String	A unique number assigned by the badge manufacturer (in badge ROM and visually readable on badge surface).
Badge Status	10 B	Binary	Specific badge status bits (each field converted into bytes).
Posting Application ID	3 B	String	Assigned identifier of application detecting event and posting record to audit log.
Event Data	51 B	String	Data specific to event (field tagged) or text explanation.

The printed audit log format will appear as follows:

```
12345678901234567890123456789012345678901234567890123456789012345678901234567890

EEE^YYYYMMDDD^HHHMMSS^UUUUUUU^WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW^BBBBBBB
BBB^SSSSSSSSSS^AAA^TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
```

4.4 Other Data Stores

BADGE STATE TABLE (multiple)

Field Name	Field Size	Field Type	Description
Badge Serial Number	4 B	Ulong	A unique number assigned by the badge manufacturer (in badge ROM and visually readable on badge surface).
Badge Status	2 B	Binary	Specific status bits (see definition below).
Time First Appearing	8 B	Datetime	Date and time the badge presence was first detection (this session)
Time Most Recently Seen	8 B	Datetime	Date and time of most recent presence detection (this session).

BADGE STATUS BITS

Field Number	Number of Bits	Field Name	Description
1	1	Reset status	True/false
2	1	Initialization Indicator	True/False
3	1	On-person (instantaneous)	1 = Currently on person 0 = Currently not on person
4	3	Removal probability (determined over time)	High value = high probability that badge has been removed from person at some time since reset. (7=definitely removed, 0=definitely not removed)
5	1	Activation indicator	1 = activated 0 = not activated
6	1	KPID inserted (instantaneous)	1 = inserted 0 = not inserted
7	1	KPID removed (determined over time)	1 = removed at least once 0 = never removed
8	1	Battery low indicator	1 = low battery (Field 9 < 4) 0 = battery OK
9	3	Battery charge level	High value = fully charged 0 = discharged
10	1	Time to live indicator	1 = TTL expired 0 = TTL not expired

KEY REPOSITORY

Field Name	Field Size	Field Type	Description
Encryption Key	16 B	Ulong	A unique number assigned by the badge manufacturer (in badge ROM and visually readable on badge surface).

This value is encrypted within the database.

INI FILE

Field Name	Field Size	Field Type	Description
Badge repositioning timeout	1 B	Integer	Length of time that the system will wait when attempting to detect the presence of a badge before timing out (default = 60 sec)
Enable battery check	1 B	Boolean	True (1) indicates that a battery check is to be performed; False (0) indicates that no check is to be attempted (default = 1).
Minimum battery charge level	1 B	Integer	Value between 0-7 indicating the minimum value for which the battery is considered to be adequately charged for activation (default = 3).
Enable on-person check	1 B	Boolean	True (1) indicates that the on-person check is to be performed; False (0) indicates that

			no check is to be performed (default = 1).
Enable on-person confidence check	1 B	Boolean	True (1) indicates that the on-person confidence check is to be performed; False (0) indicates that no check is to be performed (default = 1).
Maximum on-person/removal confidence	1 B	Integer	Value between 0-7 indicating the minimum acceptable confidence that the badge has not been removed since activation (default =3).
Enable KP badge inserted check	1 B	Boolean	True (1) indicates that the KP badge inserted check is to be performed; False (0) indicates that no check is to be performed (default = 1).
Enable KP badge removed check	1 B	Boolean	True (1) indicates that the KP badge removed check is to be performed; False (0) indicates that no check is to be performed (default = 1).
Maximum unreturned badges	1 B	Integer	Maximum number of unreturned badges allowed for a user ID before no further new badge activations are allowed (default = 3).
Badge cloaking time	1 B	Integer	Number of seconds that a present badge will be ignored for automatic CIS login purposes (default = 20).
Default time to live	4 B	Integer	Default value of badge time-to-live for a given user (hours). Default = 12 hours.
Maximum time to live	4 B	Integer	Maximum allowable badge time-to-live (hours). Default = 48 hours.
Biometric server address (primary)	25 B	String	The host name of the primary biometric server.
Biometric server address (secondary)	25 B	String	The host name of the backup biometric server.
Biometric database name	25 B	String	Name of authentication database.
Failover timeout	1 B	Integer	Timeout period after making a request to the primary server and re-initiating that request to the secondary server. In milliseconds (default = 1000).
Password update timeout	1B	Integer	Length of time between failed auto login and successful manual login, within which a password update attempt will be performed (in seconds). Default = 20 seconds.
Enable auto logoff	1B	Boolean	True (1) = enabled False (0) = disabled Default = 0.
Entrust ini filename	12 B	String	Name of file to be used to setup entrust interface.

ENVIRONMENTAL INI FILE (may be combined with above)

Field Name	Field Size	Field Type	Description
Flicker filter period	1 B	Integer	Time period (in milliseconds) within which a loss of badge detection is considered an

			anomaly and is not reported as a badge departure. Default = 3000 ms.
Base Station Sensitivity	1 B	Integer	HP badge only. Sensitivity setting for IR receiver.
Base Station Receiver Attenuation	1 B	Integer	RFID only. Setting for base station RF receiver attenuation.
Badge Power Setting	1 B	Integer	HP badge only. Transmitter power output setting.
Retransmission Retry Counter	1 B	Integer	RFID only. Maximum number of retries when transmission errors are detected.
Visible Timeout	1B	Integer	
Lost Badge Timeout	1B	Integer	

BADGE INI FILE

Field Name	Field Size	Field Type	Description
Badge serial number #1	4 B	Ulong	Serial number of RFIDeas badge in inventory (for polling list).
Badge serial number #2	4 B	Ulong	Serial number of RFIDeas badge in inventory (for polling list).
Badge serial number #N	4 B	Ulong	Serial number of RFIDeas badge in inventory (for polling list).
Badge polling interval			Time between successive polls (ms), (default = 100).

LOGIN STATE TABLE

Field Name	Field Size	Field Type	Description
Login state	1 B	Integer	1 = Ready 2 = Busy 3 = Wait
Current login ID	7 B	String	User ID of currently logged in user. Blank if no user logged in.
Current login badge	4 B	Ulong	Serial number of badge currently logged in. Blank if no user logged in.

LOGIN CANDIDATE LIST (multiple) (may be combined with above)

Field Name	Field Size	Field Type	Description
User ID	7 B	String	A unique string value consisting of a beginning alpha character followed by 6

			numeric characters.
Badge number	4 B	Ulong	A unique number assigned by the badge manufacturer
Cloaking indicator	1 B	Boolean	0 = not cloaked 1 = cloaked
Cloak start time	4 B	Long	Time when cloaking began.
Notification indicator	1 B	Boolean	Indicates whether the application has been notified of this user. 0 = not notified 1 = notified
No-login indicator	1 B	Boolean	Indicates if badge is on no-login list. 0 = not on list 1 = on list

NO-LOGIN LIST (may be combined with above)

Field Name	**Field Size**	**Field Type**	**Description**
User ID	7 B	String	A unique string value consisting of a beginning alpha character followed by 6 numeric characters.
Badge number	4 B	Ulong	A unique number assigned by the badge manufacturer
No-login reason	1 B	Char	1 = User logoff (cloak time applies) 2 = Failed auto login (reset when departure detected) 3 = Bad badge status (reset upon departure) 4 = Badge revoked (reset upon departure) 5 = Bad syntax check (reset upon departure)

5.0 Security and Availability

This section describes the security and availability requirements for the system.

5.1 Security Features

Security features fall into 2 primary categories, which are described in the following sections.

- Access control
- Encryption

5.1.1 Access Control

Access controls prevent access by unauthorized personnel or software entities. Access controls will be provided for the following:

- Authentication administration application. Only BARB subsystem administrators may access this application to protect against unauthorized personnel performing user and badge management functions. BARB subsystem administrators will be biometrically authenticated to access this application. A backup password access mechanism will also be supplied.

- Authentication database access. Access to the biometric/badge database will be password protected.

- Badge data access. Access to data uploaded to a badge will be password protected. Passwords include a global password and individual data field passwords. For the pilot system, a single password will be utilized and will be hardcoded within the reading/writing application.

All password data must be purged when its immediate use has been completed.

The BARB subsystem provides a user authentication facility for CIS as described in Section 2. The BARB subsystem does not provide CIS with any authorization capabilities (access controls are determined by CIS).

5.1.2 Encryption

Encryption of sensitive data is required for confidentiality and integrity purposes. The following data will be encrypted:

- All biometric data transmitted between platforms (i.e., client/server communications) will be encrypted. The Windows Crypto API will be used wherever possible. Client/server

communications will be encrypted using RSA RC4 128-bit encryption with session keys, using Diffie-Hellman key exchange. Secure RPC also provides mutual authentication of sender/receiver.

- Biometric data stored within the authentication database by the Biometric Server will be encrypted prior to transmission and storage using symmetric RSA RC4 128-bit encryption. All symmetric keys will be randomly generated and securely stored (encrypted). Multiple levels of protection is preferred.

- Data transmission to/from the badge will be encrypted if supported by the underlying badge technology.

- All application data will be encrypted by the BARB subsystem before being sent to the badge.. Encryption keys will be randomly generated and securely stored (encrypted) on the central server. These keys will be distributed only to authorized applications (shared secret). Secure transmission will be used (secure RPC).

Strong encryption (128 bit keys) will be used. Secret and private keys will be protected from compromise. Any distribution of keys will use secure mechanisms. Key escrow (for the biometric database) will be provided.

A mechanism of synchronizing keys between the redundant biometric/database servers will be provided. Once the encryption key has been generated on the primary server, a utility will be provided to move that key to the secondary server(s). This mechanism involves writing the key to a floppy disk at the primary server and reading it at the secondary server. Once created, the floppy disk containing the encryption key will serve to provide a key escrow mechanism for use in restoring the BARB system should a major failure occur (e.g. concurrent registry corruption on both biometric servers, etc.). The floppy disk will be given to Kaiser administrative personnel who will be responsible for storing the encryption key escrow disk in a secure location.

[Future - periodic key changes will be accommodated.]

5.2 System Availability Features

The biometric server and database must be implemented redundantly with automatic failover capability to avoid this being a single point of failure. For the pilot, this will be accomplished using dual SAFservers and SQL Server replication, with client initiated retries, as shown in Figure 28, below.

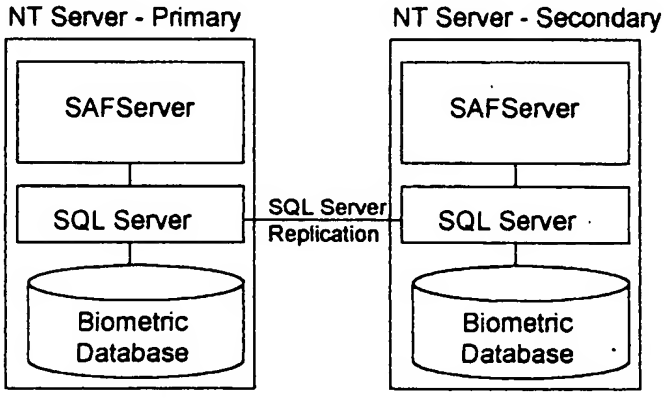


Figure 28. Server Replication Configuration

Two SAFServers are set-up using SQLServer replication. In this case, one server is the primary (or publisher) of the information and the other is the secondary (or receiver) of the information. In this case, at pre-defined intervals, the biometric database is automatically "replicated" from the primary to the secondary database (initially, the entire database is replicated, then only changes between intervals).

In this case, the client is aware that two (or more) SAFServers exist. If, after a pre-defined timeout, the primary server fails to respond to a request, then the client assumes that a failure has occurred and sends the same request to the secondary server.

Replication is a standard part of SQL Server. It does require a fair amount of expertise to configure properly. Note also that since the SAFServer encrypts the biometric data prior to storing it within the SQL database, part of the configuration involves sharing of the encryption keys between the primary and secondary servers.

[Future - for the operational system, IBM Secureway will be used to provide 3rd party failover and load balancing capability.]

To ensure that the user may always access the CIS system, even in the event of a badge or authentication system failure, the existing manual user ID/password entry capability must continue to be available as a backup and to accommodate non-pilot participants.

During the pilot, two biometric technologies will be available for enrollment and authentication. If the user fails to authenticate on one, he should have the capability of using the other.

The system must be able to accommodate multiple Administration and A&A stations, although these may not be implemented during the pilot rollout.

6.0 Future requirements

The following is a list of known/anticipated future system requirements. These will not be implemented in the pilot; however, where possible, accommodations will be made to allow for such upgrades in the future.

- User aliases
- App driven policies
- 3rd party failover/load balancing
- Programmed API for data upload/distribution
- Security features - admin logon, mutual authentication, trusted path
- SAF/nt for initial workstation boot/network logon + at physicians desks
- Badge removal detection (now?)
- Audit of who in room at any time, where are all badges presently located
- Badge deactivation/reactivation by user (deactivation now?)
- Auto logoff (when leave room)
- Complex security policies with context and state
- Incorporate user groups
- Periodic DB encryption key changes
- More sophisticated key distribution
- BioAPI compliance
- BSP improvements - indicate which fingers/eyes enrolled, allow update of single template
- More secure channel between badge interface and badge SDK
- Reading/writing of large data blocks to badge, in chunks
- Asynchronous read/write to badge SDK (NT service)
- Use of badge advanced features (speaker/mic, LEDs, etc.)
- Utilize Unix biometric server
- Use open system enterprise database - Oracle

Sample

TagSense

Wireless Identification and Data Interface

Submitted to:

Kaiser Foundation Health Plan
393 E. Walnut St.
Pasadena, CA 91188

Submitted by:

TagSense, Inc.
432 Columbia St., Suite B13B
Cambridge, MA 02142
Tel: (617) 494-1001
FAX: (617) 494-6006

EXHBIT C

I. Introduction and System Overview

The Wireless Identification and Data Interface (WIDI) system is being built for Kaiser Permanente to provide automatic identification and small-scale data transport services. It is understood that the interest of Kaiser Permanente is to test the applicability of such a system in a medical/healthcare setting. The primary goal of this application is to increase security levels for information levels while services, while easing the operational burden on the user by reducing the dependence on use of usernames and passwords within medical information systems and extending the current ease of use provided by conventional magnetic stripe and RFID access control badges into the realm of medical information systems.

The system is targeted to allow physicians and other healthcare providers in various locations easy and rapid secure access to medical information applications by providing alternative credentials (to the conventional username and password) that will identify and authenticate the provider. This functionality will simplify centralizing identification and authentication records, and will minimize the need for wide spread access to such centralized records by providing authentication credentials that travel with the provider. By providing the ability to transport small amounts of relevant data with the human user, the WIDI system can also simplify working situations in the absence of network connectivity.

The WIDI system is comprised of 3 main elements:

The first element, which provides the identification, authentication and data transport services, is a badge device. The badge has 2 communication channels on board, one radio frequency link (RF) that provides long-range (room scale), low speed communication, while the other is an infra-red (IR) link that provides short-range (few feet), high-speed communication as well as field of view (FOV) detection. The badges are equipped with a small amount of memory that can be used to transport arbitrary data. In addition, the badge includes lights and a small sound beeper to provide feedback to the user and a simple sensor to help detect when the badge has been removed. In addition, the badge contains a holder for a traditional Kaiser-Permanente ID badge, which can be used to add an additional level of system security.

The second element is the base stations, which are the interface between the badges and the computer workstations running the application software. The base stations also have RF and IR links to communicate with the badges, and they communicate with the workstations through the serial communications port on the computer platform.

The third element is a software SDK, written in the C++ programming language, that will be used by the applications that are enabled to use the system to communicate with the base station and to access the services provided by the system.

Each of these subsystems are described in greater detail in the sections below.

II. Scope

It is the understanding of Tagsense, Inc. that the WIDI system is intended to be a part of a larger prototype system that Kaiser Permanente is developing for the medical/health care field. This scope of this proposal and the scope of the ensuing contract between TagSense and Kaiser Permanente is limited to the short term development effort of the relevant prototype hardware and a software SDK. Due to the very short time frame of this effort, and the development risk involved, the specifications listed in the Statement of Work are conservative.

In this phase of the development effort, it is understood that the *primary* objectives are:

- to create a prototype that provides the basic technical functionality that will enable users to evaluate and to understand the overall concept of the intended application
- to create a prototype that conveys "the look and the feel" of the application system concept

In addition to these objectives, it is understood that there exist longer-term objectives which would be relevant and necessary for future product development but are not essential for initial testing and evaluation. These objectives include:

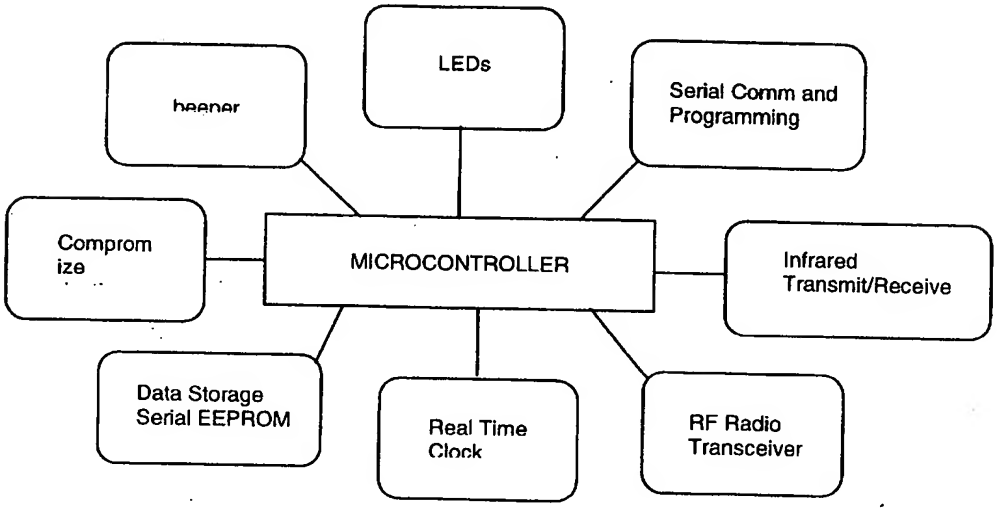
- optimizing the battery life of the badges
- optimizing the small size and weight of the badges and base station
- optimizing the detection angle and range of the infrared and/or RF subsystems
- optimizing the security countermeasures and encryption level of the system
- evaluating and ensuring compliance with FCC regulations

Due to the extremely short development time, it is understood that the scope of this contract shall be limited to satisfying and meeting the primary objectives listed above.

III. Statement of Work

The following sections describe the basic specifications of the system.

Badge Hardware



Badge components

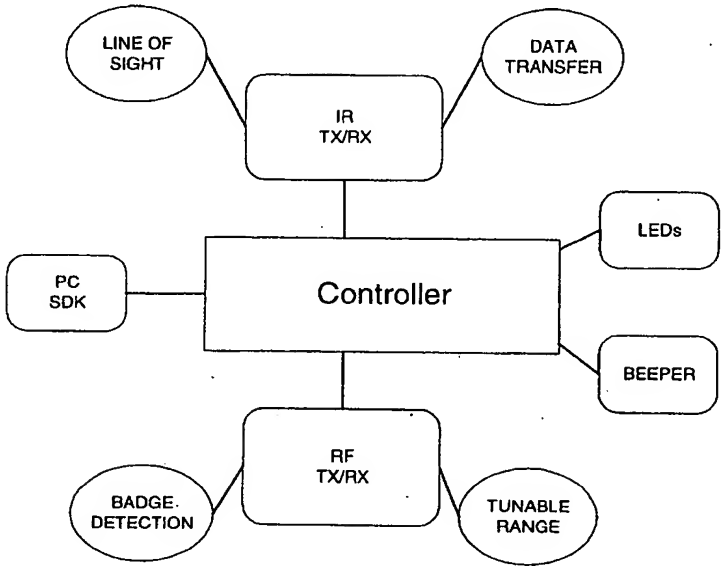
The role of the WIDI badge is to communicate with the base station, to identify itself and its status, to store a certain amount of data (e.g. credentials and badge health parameters), and to provide some task-related feedback to the user in the form of simple lights and an audible tone.

TagSense shall provide 30 badges which include the following features:

- RF communication (9600 baud nominally)
- RF range can be electronically adjusted over at least 2 settings
- Infrared communication (>9600 baud)
- 16 or more Kilobytes of data storage
- Real-Time Clock module
- Support for a "time-to-live" setting which establishes a lifetime for badge resident user data. Upon expiration, the badge will self-erase all user data.
- LED and beeper for user feedback
- At least 16 hours battery life
- Battery-powered (a variety of battery options will be explored to help minimize size and weight of the badge.

- option for tethered reprogrammability/communication via PC
- There will be a unique number assigned to each badge (digital identifier)
- Contact sensor to determine if a traditional ID Badge is inserted in the badge holder. The badge will have no means of verifying that the object placed in the badge holder is indeed an authentic ID badge.
- limited spoof protection to safeguard against man-in-the-middle and playback attacks.
- Capacitive sensor to be used as a possible means to help determine the removal of the badge from a user
- The ability to notify the base station of state changes in one or more of the onboard sensors

Base Station Hardware



WIDI Base Station components

The base station is the interface between the badges and the rest of the system. The base station has four major features IR communication, RF communication, user feedback, and interface with the SDK. The basic function of the base station is to communicate information to and from the badges through IR and RF data links. Additionally, the base station shall detect if a given badge is within line of sight (a.k.a. "sight detection"). It is assumed that the base station shall be connected to a computer.

TagSense shall provide 15 base stations that include the following features:

- IR Link for the purpose of sight detection and data transfer. Each badge may emit an IR refresh signal at some frequency to be specified. Secondly, the refresh signal also provides a means by which the line of sight detection can be effected.

- RF link for badge detection and badge identification. Assuming parts availability, the operating frequency in the range of 433 MHz shall be used. This frequency is a common standard for commercial wireless devices and is a good trade-off between high frequency (data rate, bandwidth) and low-frequency (RF penetration, resistance to human shielding effects).

- A discovery algorithm which enables the system to detect new badges which enter within RF range of the base station. Although in theory this discovery process can be used to enable support for an arbitrary number of badges, in practice, the number of badges is limited by user requirements for system update rate and limited by certain special cases, such as a number of badges entering the RF range simultaneously.

- The base station will be able to uniquely identify and communicate with at least four badges within the RF range. The system will continue to communicate reliably with these pre-existing badges if more badges enter the area within RF range.

- The base station will have an electronically tunable range over at least 3 settings, where one of the settings is no output.

- The user feedback will be done using LED's and a beeper. The purpose of the feedback is to let the user know if a download/upload or login is in progress, successful or unsuccessful. Application access to the LED's and beeper functions will be exposed throughout the SDK

- The base station is connected to the computer through the serial port at 9600 baud or greater.

- The IR field of view of the base station will be at least 30 degrees to the left and right of the center of the base station.

Software SDK

The software SDK will provide the means of interaction between the Kaiser applications and the system. The SDK will be written as a Windows dynamic linked library (DLL) that will provide library calls implementing the various

levels of functionality. The most basic level of functionality will be the transfer of arbitrary encoded data to and from a device connected to the serial port; this data will include both instructions for the base station connected to the serial port, and instructions and data for onward transmission to one or more badges. The functions provided by the SDK will utilize this functionality to send commands and provide the identification, authentication and data transport services to the applications that use the SDK.

- The ability to set up a particular badge (e.g. reset, determine status, write user data, set "time to live", etc.).

- Data management will be done by the badge. Each user data element will consist of three parts: data tag identifier, data value, and access password. The SDK will support the reading, writing and deletion of individual data elements. The SDK will support a "delete all" function protected by a global password. It should be noted that this data structure was proposed by Kaiser Permanente and it is acceptable by TagSense for the prototype; however, in general, it is not good design to transmit passwords, and implementing a challenge-response scheme for data access is preferred.

- Support for event notification: programs should be able to request notification of events such as a specific badge entering or leaving either RF or IR range of a base station, as well as continuous keep alive signals (indicating that a specific badge is still in range of the base station).

- System enumeration functions, to allow a count to be taken of all the badges within RF or IR range of the base station, with a minimum of 5. Typically the IR enumeration will be directional and will provide a field-of-view (FOV) count that can be used to determine whether or not a badge is within line-of-sight to a specific monitor.

- Ability to detect compromise history of a particular badge. The badges will use a sensing technique to provide reference information about whether or not a badge has been removed. The SDK will provide functions to let an application retrieve and modify this information in real time.

- Integrated into the device will be limited safeguards against RF and IR replay, and man-in-the-middle attacks. A random message sequence ID number scheme will be adopted as the limited safeguard against replay attacks, and a time-stamp and message request timeout will be adopted as the limited safeguard against man-in-the-middle attacks. Protection against eavesdropping will not be implemented for the prototype, since the only effective defense against eavesdropping is a strong encryption algorithm for the RF/IR transmissions, which requires development beyond the scope of this contract.

- Software will be written in C/C++

- It is assumed that the user data received by the SDK /SDK will already be encrypted, so no additional encryption will be provided.

IV. Packaging

Packaging of the prototype WIDI hardware is critical in order to provide ease of use and to enable use of the hardware in a realistic setting. If the prototype system is to be evaluated by "real-world" users at some future date, proper and robust packaging of the badge and base station are necessary, not merely for aesthetic reasons, but are simply needed to make the system usable.

TagSense shall provide the following packaging features for the badges:

- robust design
- attention to minimizing size and weight with maximum size not exceeding 3.5" X 4.5" X .75" and weighing no more than 5 oz including batteries. These numbers are very conservative, but permit a variety of form factors and battery options to be explored.
- attachment method to ensure IR communication and ease of removal
- Splash-resistant sleeve
- Accommodation (holder) into which user can insert existing name badge
- Aesthetically pleasing appearance

TagSense shall provide the following packaging features for the base stations:

- robust design
- attachment method to computer monitor which ensures communication with badge and ease of use with the goal of being as unobtrusive as possible.
- Splash-resistant casing
- Minimum-size form factor with aesthetically-pleasing design

V. Resources

Facilities

TagSense has 300+ sq ft of commercial office space located at 432 Columbia St. in Cambridge, MA. This lab contains all the necessary equipment for design, testing, and assembly of the electronics hardware. Fabrication of the actual printed circuit board shall be done by an external board fab house, which is standard practice in the industry. Fabrication of the electronics packaging and plastic housing will require some use of external resources such as a laser cutter and machine shop which Tagsense shall lease hourly in the local area. To save time on the electronics assembly for the multiple circuit boards, TagSense will also hire an external assembly service at a rate of $26/hour to assist with the soldering.

Personnel

Rich Fletcher (project management, badge hardware):
Mr. Fletcher is currently completing his PhD thesis at the MIT Media Lab wth emphasis on low-cost electromagnetic identification and sensing systems. Mr. Fletcher holds bachelor degrees in Electrical Engineering and Physics from MIT as well as a Master's Degree from the MIT Media Lab. His past experience includes research in wireless sensors, short-range wireless electronics, and passive microwave devices as an officer in the US Air Force.

Kenroy Cayetano (base station hardware):
Mr. Cayetano is currently a research assistant at the McLean Hospital Brain Imaging Center. He received the Minor Degree in Mechanical Engineering and the S.B degree in Electrical Engineering and Computer Science from MIT in 2000 and is currently completing a Masters of Engineering, with thesis work on Magnetic Resonance Imaging hardware. His interests and research include MRI RF receiver coil design, and analog and digital circuit design.

Steve Gray (Embedded code - firmware):
Mr. Gray has an S.B. degree from MIT in Electrical Engineering and Computer Science and a Master's Degree from the MIT Media Lab. Mr. Gray specializes in developing firmware for low-power wireless networks, and has worked as a consultant on several projects, including telemetry systems for the European Motorcycle Grand Prix and the climbing expeditions to Mt. Everest. His most recent project is a portable wireless telemetry system for the US Army for monitoring the physiological parameters of field soldiers in real time.

Olufemi Omojola (Windows software, SDK):

Mr. Omojola is currently a research assistant in the Physics and Media Group at the MIT Media Laboratory. He received the S.B. degree in electrical engineering and computer science from MIT in 2000 and is currently completing a Masters of Engineering. Mr. Omojola served as a 3-year summer intern at Microsoft Corporation developing Windows database systems and software packages such as Microsoft BackOffice. His interests include flexible reconfigurable hardware architectures for signal processing and applications for human-computer interfaces.

Kelly Heaton (industrial design, fabrication):

Kelly Heaton is a designer with a background in art and science. She received her Bachelor's degree in Ecology and Urban Planning from Yale University (1994) and her Master of Science from the MIT Media Laboratory (2000). She has also conducted post-graduate research at the School of the Museum of Fine Arts, Tufts University and the College of Veterinary Medicine at North Carolina State University. She has received numerous grants and fellowships for her work in visual art, including the prestigious Jacob K. Javits Fellowship. Her research at the MIT Media Laboratory has been presented at SIGGRAPH (1999) and can be seen on the web at: http://www.media.mit.edu/~kelly. Heaton is a current recipient of an individual artist's grant from the MIT Council for the Arts and a Research Affiliate of the Center for Advanced Visual Studies at MIT. Ms. Heaton has worked on a number of industrial design projects, including design and fabrication of prototypes for the toy industry.

VI. Schedule

The schedule for this project is six weeks, with system scheduled to ship on or before Saturday, November 4, 2000. This is an extremely aggressive schedule, given the number of units that need to be produced and hand-assembled.

VII. Cost Proposal

The primary factors determining the cost are the following:

- very aggressive schedule
- number of units that need to be hand-assembled (30 badges, 15 base stations)
- royalty-free license to Kaiser-Permanente for production of future units

The following is our cost proposal:

Engineering:	
$65/hr X 25 hrs/week X 6 weeks = $9750/person X 4 people =	$39,000
Packaging design, fabrication, machining:	
$65/hr. X 40 hrs/week X 3 weeks X 1 person =	$10000
Electronics assembly service:	
$26/hr X 40hrs =	$1500
Printed circuit board fabrication service:	$10500
Electronic components and radio modules for 30 badges, 15 base stations	$3000
Packaging/housing materials/hardware:	$1500
Machine shop/laser cutter leased time:	$3000
Administrative/lawyer fees:	$1000
TOTAL:	**$69,500**

TagSense requests a deposit/retainer fee of $15,000 to cover initial parts procurement and set-up costs, with the balance to be paid in full upon delivery of the proposed system. Travel costs will be reimbursed separately by Kaiser Permanente and are not part of this contract.

VIII. Additional Terms

TagSense and Kaiser Permanente shall use good faith in including the terms of this proposal, and certain additional terms customary for this type of arrangement, in the binding agreement. Additional terms are the following:

Acceptance and Approval:

To mark completion of the contract, TagSense agrees to deliver 30 badges, 15 base stations, and a software SDK with specifications meeting or exceeding what is specified in this proposal. Payment to TagSense is expected shortly thereafter.

In addition to the deliverables stated above, TagSense agrees to supply Kaiser Permanente with the necessary materials and information needed to copy the prototype. These materials are:

- CAD files (gerber format) for the circuit boards for the badge and base station
- Firmware hex files used to program the microcontroller on the badge and the base station
- CAD files and drawings for the badge and base station packaging
- Bill of materials (i.e. parts list)

In addition, TagSense also agrees to provide the following:

- Circuit schematics for the badge and base station
- Source code for the software SDK
- Brief (2-3 pages) written instructions describing the use of the badge, base station, and SDK.

The source code for the firmware will not be provided under this contract since it is not required for making additional copies of the prototype system and since it contains a large amount of pre-existing intellectual property that TagSense does not wish to disclose at this time. The firmware hex files are sufficient for the purpose of making additional copies of the prototype.

Parts Availability:

Due to the short time period of this contract, parts must be procured in a timely manner. Tagsense will procure parts as soon as the initial retainer fee is received. TagSense has already investigated the ordering availability of the parts required for this project as of Sept 13, 2000. However, parts availability is always subject to change. Should a required part become unavailable, TagSense shall procure an appropriate substitute. If this change will result in

any significant change to the system specifications, TagSense will let this be known to Kaiser Permanente.

Post-contract support and warranties:

In order to meet the needs of Kaiser Permanente for test and evaluation, a significant amount of design effort shall be devoted to making the hardware physically robust and user-friendly. Nevertheless, it is to be understood that system to be developed is a working prototype with its primary goal being to demonstrate functionality.

TagSense will make a best effort to minimize the cost of the badge and to maximize its manufacturability. Due to the tight deadline and space constraints on the badge, integrated radio modules will be used for this design, which cost approximately $15 each in quantities of one thousand. After the testing of the system by Kaiser Permanente, it may be possible to replace this radio module with a low data rate cheaper discrete parts radio at the expense of increased badge size and increased complexity. TagSense will consider a follow-on task to further explore design options and to continue development of the system.

For the six-month period following delivery of the system to Kaiser Permanente, TagSense agrees to the following included in the cost of the contract:

- Reasonable amount of telephone support for technical questions (for example, 2 calls per week or less)
- Hardware repair. Kaiser Permanente will cover shipping costs. Units that have been abused or physically damaged by users are not covered.

Following the six month period, TagSense will consider a service agreement with Kaiser Permanente to continue repair/maintenance of hardware.

Intellectual Property:

Upon completion of the contract, TagSense shall retain the right to all pre-existing intellectual property (e.g. wireless hardware, firmware, electronics know-how) used in this project. TagSense reserves the right to continue using such intellectual property, with the exception of application-specific Intellectual property covered under the Non-Disclosure Agreement between TagSense and Kaiser Permanente. TagSense will retain full rights to the design created under this contract until final payment is received from Kaiser Permanente. Upon completion of the contract and receipt of payment, Kaiser Permanente shall be granted non-exclusive non-transferable royalty-free rights

to the specific hardware and software developed under this project for sole use in the intended application discussed for this project.

Liability:

TagSense has no knowledge of and makes no claims regarding the usability or suitability of this hardware for this application. TagSense is developing this hardware to match the specifications set forth by Kaiser Permanente and shall not be liable for any potential future legal claims set forth against TagSense or against the systems developed under this contract.

Example API for Kaiser Badge

```
Result := GetAPIVersion();
Result := GetBadgeVersion();
Result := ResetTheBadge(BadgeNumber TimeToWait);
Result := SetBadgeAccessPassword(BadgeNumber, Password);
Result := InitializeTheBadge(BadgeNumber, Password);
Result := SetExpirationTime(BadgeNumber, Password, ExpirationTime);
Result := GetExpirationTime(BadgeNumber, Password);
Result := SetBadgeRFPower(BadgeNumber, Password, Power);
Result := GetBadgeRFPower(BadgeNumber, Password);
Result := SetBaseRFPower(Power);
Result := GetBaseRFPower();
Result := SetBadgeIRPower(BadgeNumber, Password, Power);
Result := GetBadgeIRPower(BadgeNumber, Password);
Result := SetBaseIRPower(Power);
Result := GetBaseIRPower();
Result := SetBadgeStatus(BadgeID, Password, Status);
Result := GetBadgeStatus(BadgeID, Password);
Result := GetBadgesInView(BadgeList);

Result := WriteToBadge(BadgeID, Password, DataIdentifier, DataPassword
, Data, Length);
Result := ReadFromBadge(BadgeID, Password, DataIdentifier, DataPasswor
d, Data, Length);
Result := DeleteDataFromBadge(BadgeID, Password, DataIdentifier, DataP
assword);
Result := DeleteAllData(BadgeID, Password);

Result := SetSystemTime(BadgeID, Password, Hours, Minutes, Seconds);
Result := GetSystemTime(BadgeID, Password, Hours, Minutes, Seconds);

Result := SetBadgeLEDs(BadgeID, Password, LEDMASK);
Result := GetBadgeLEDs(BadgeID, Password, LEDMASK);
Result := SoundBadgeBeep(BadgeID, Password, Frequency, Duration);

Result := SetBaseLEDs(BadgeID, Password, LEDMASK);
Result := GetBaseLEDs(BadgeID, Password, LEDMASK);
Result := SoundBaseBeep(BadgeID, Password, Frequency, Duration);
```

****

```
long SetVisibleTimeout(long VisibleTimeout);
long GetVisibleTimeout();
long SetLostBadgeTimeout(BadgeID ID,
                         long Lost_Timeout,
```


EXHIBIT D

```
                        long MaxDelay,
                        void *GlobalPassword);
long GetLostBadgeTimeout(BadgeID ID,
                        long MaxDelay,
                        void *GlobalPassword);

long GetEnumerationSize();
long GetEnumerateBadges(pEnumeratedBadges pBadges,
                        long Size,
                        long *ActualSize);



long DataItemAsyncWrite(BadgeID ID,
                        long Tag,
                        long Length,
                        void *data,
                        long MaxDelay,
                        void *Password
gs TBD                                          //,    // the followin

                        //CallBackFunction,
                        //...
                        );

long DataItemGetSize(BadgeID ID,
                     long Tag,
                     long MaxDelay,
                     void *Password);


long DataItemAsyncRead(BadgeID ID,
                       long Tag,
                       long Size,
                       void *Data,
                       long *ActualSize,
                       long MaxDelay,
                       char *Password
                                        //,  // the following TBD
                       //CallBackFunction,
                       //...
                       );

long DataItemsGetNumber(BadgeID ID,
                        long MaxDelay,
                        void *GlobalPassword);
```

```
long DataItemsEnumerate(BadgeID ID,
                        long Size,
                        long *Tags,
                        long *ActualSize,
                        long MaxDelay,
                        void *GlobalPassword);
```

VIDEO SCRIPT

TITLE: **"BARB Test Announcement"**

PREPARED FOR: **Kaiser Permanente**

PRODUCTION #: **5951**

WRITER: **Teri Allen (818-243-6785)**

PRODUCER: **Jo Ann Lesser**

DRAFT : **11**

DATE: **May 9, 2001**

EXHIBIT E

FADE IN:

1. OPEN WITH SEVERAL VERY CLOSE SHOTS OF THE BARB. WITH EACH SHOT, WE REVEAL MORE AND MORE

VOICE OVER NARRATOR: It measures about 3 by 4 inches. It weighs just an ounce and a half. It's so light you barely know it's there.

2. WE NOW SEE A SHOT OF BARB FULLY REVEALED (IT COULD BE HELD IN SOMEONE'S HAND. THEY FLIP IT BACK AND FORTH SO WE SEE BOTH SIDES, INCLUDING ALL THE ELECTRONICS)

It's called the BARB and it's going to make your life a lot easier.

3-6. OMIT

nA : MCF

7. TRANSITION TO CLOSE SHOT OF THE BARB, NOW ATTACHED TO A PHYSICIAN'S ID CARD. THEN CUT TO OVER-THE-SHOULDER SHOT OF A PHYSICIAN AT A COMPUTER TERMINAL

The BARB is a small electronic device used in conjunction with Kaiser Permanente's new Clinical Information System -- or CIS.

7A. START THIS SEQUENCE WITH A CLOSE UP OF THE BARB, THEN CUT TO SCREEN SHOTS AS THE CIS LOG-ON PAGE APPEARS (WITH USER ID AND PASSWORD ENTERED); CIS MAIN MENU APPEARS

BARB enables you to access CIS *without* having to use a password every time you log on. Kaiser Permanente is currently testing the BARB prototype and here's how it works.

8. TRANSITION TO BARB 'ENROLLMENT' AREA - SHOW BRIEF SEQUENCE OF EVENTS AS OUR "PHYSICIAN" IS BEING MEASURED FOR FINGER AND/OR IRIS SCAN

During a one-time enrollment process, we'll scan your finger or take a picture of your eye. These measurements are unique to you and some of the characteristics are stored to be used to verify your identity.

9. BARB 'PICK UP' AREA - START WITH CLOSE SHOT ON A BOX OF BARBS. PULL OUT AS OUR PHYSICIAN ENTERS THE AREA, PICKS UP A BARB AND SLIPS IT ON HIS EMPLOYEE ID **SHOOT WITH ASSIGNED BARB TOO**

(1) Then, every time you come to work, you'll pick up a BARB in a designated area and attach it to your ID card. At this point, the BARB is blank, with no data linking it to you or anyone else.

10. ANOTHER ANGLE AS OUR PHYSICIAN GOES TO COMPUTER TERMINAL TO SIGN-IN. SHOW SCREEN THAT REQUESTS ENTRY OF THE BARB/BADGE NUMBER

(2) Next, during a brief computerized sign-in procedure, you'll (2a) be prompted to enter your BARB's ID number.

10A. CLOSE SHOT OF BARB BADGE AS PHYSICIAN TURNS IT OVER TO SEE ID NUMBER

You'll find it on the back of your BARB badge.

10B. CLOSE SHOT OF COMPUTER SCREEN AS PHYSICIAN ENTERS BADGE NUMBER

10C. REMAIN CLOSE ON COMPUTER SCREEN AS PHYSICIAN ENTERS USER ID AND PASSWORD

(b) You'll also be asked to enter your user ID and password.

10D. REMAIN CLOSE ON SCREEN AS WE SEE "PLEASE PLACE YOUR FINGER ON THE FINGER LOCK SENSOR." INCLUDE SHOT OF PHYSICIAN PLACING FINGER ON THE SENSOR

(c) Then we'll either scan your finger and compare the results to the data taken earlier and stored in the system...

10E. ALSO SHOW SEQUENCE ON THE SCREEN IN WHICH WE SEE A REQUEST FOR "IRIS RECOGNITION" AND THE PHYSICIAN TAKING AN IRIS SCAN

(a) ...or we'll use iris recognition to verify your identity.

10F. SHOT OF "ACTIVATION SUCCESSFUL" SCREEN (WITH EXPIRATION TIME)

(3) Once that's done, the BARB you're wearing is automatically activated and will remain active until the expiration time shown on the screen.

10G. ANGLE AS OUR PHYSICIAN LEAVES THE SIGN-IN AREA AND HEADS FOR HIS/HER OFFICE	That's all you have to do. Everything else happens behind the scenes.
11. MOVED AFTER 15A	
12. INT - PHYSICIAN'S OFFICE. ANGLE AS THE PHYSICIAN ENTERS THE OFFICE AND SITS AT HIS/HER COMPUTER. WE SEE THE BASE STATION	Now, when you go to your office or an exam room, you'll see a small base station next to the computer terminal.
12A. START WITH SHOTS OF LIGHTS BLINKING ON THE BASE STATION. ALSO CLOSE SHOTS OF THE BARB. THEN SCREEN SHOTS OF THE CIS LOG-ON SCREEN BEING OPENED. WE SEE USER ID AND PASSWORD, THEN CIS MAIN MENU APPEARS	(1) The station detects your BARB, (2) notifies the system that you're in the area and (3) automatically opens the CIS log-on screen. (4) The system automatically enters your user ID and password, (3) then goes to the CIS Main Menu. You can open many menu items without having to enter a separate password for each one.
12B. SHOW PHONE MESSAGES SCREEN	For example, you can retrieve your phone messages.
12C. SHOW PATIENT INFORMATION SCREEN	Or you can call up patient information.
12D. CLOSE SHOT OF THE PHYSICIAN HITTING F3 ON THE KEYBOARD. THE PROGRAM LOGS OFF. PHYSICIAN LEAVES HIS/HER OFFICE	(6) When you leave your office, it's easy to log off so an unauthorized person can't change or see any confidential information.
13. INT - EXAM ROOM. PHYSICIAN ENTERS THE EXAM ROOM, GREETS PATIENT SITTING ON EXAM TABLE AND APPROACHES COMPUTER TERMINAL	In each exam room you enter throughout the day, BARB makes logging on to CIS just as quick and easy.

13A. CLOSE SHOT ON COMPUTER AS CIS LOG-ON SCREEN APPEARS ALONG WITH USER ID AND PASSWORD. CIS MAIN MENU APPEARS

Simply approach the computer and the CIS log-on screen appears. Each time, your user ID and password are automatically entered with no action on your part.

13B. SCREENS SHOWING PATIENT INFORMATION AND LIST OF MEDS SCREEN

Once you're in CIS, you can access patient information or a list of medications your patient is taking *without* having to enter a separate password.

14. CLOSE SHOT OF THE PHYSICIAN HITTING F3 ON THE KEYBOARD. THE PROGRAM LOGS OFF. (WE SEE THE PATIENT LEFT ALONE IN THE EXAM ROOM. THE PATIENT REMAINS SEATED ON THE EXAM TABLE, BUT WE SEE HIM/HER TRYING TO SEE WHAT'S ON THE COMPUTER SCREEN)

After you're finished using the computer, a single key stroke logs you off.

14A. INT - SAME EXAM ROOM, LATER. MEDIUM SHOT IN SAME EXAM ROOM WITH A DIFFERENT PHYSICIAN (WEARING A BARB) AND PATIENT. PHYSICIAN APPROACHES THE SCREEN. SCREEN SHOTS AS WE SEE THE CIS LOG-ON SCREEN WITH THE USER ID AND PASSWORD ALREADY FILLED IN. THEN CIS MAIN MENU APPEARS

Later, when another physician uses the same exam room, his or her BARB will also automatically open the CIS log-on screen and enter the user's ID and password. With BARB, it's that easy to call up CIS time after time...user after user.

14B. SEVERAL OTHER QUICK SHOTS OF SEVERAL PHYSICIANS ENTERING VARIOUS EXAM ROOMS AND THE CIS LOG-ON SCREEN AUTOMATICALLY BEING PULLED UP TIME AFTER TIME

When you think of all the times you and your colleagues will be accessing the Clinical Information System during the day, BARB is definitely a convenience and a time saver. Without BARB, you'd have to type in your user ID and password every time you entered a new exam room or office and logged onto CIS.

14C. SCREEN SHOT OF THE CIS LOG-ON SCREEN WITH USER ID AND PASSWORD FILLED IN

Instead, BARB recognizes you and signs you in.

14D. SHOT OF PHYSICIAN AT COMPUTER ACCESSING CIS PROGRAMS. WE SEE THE PATIENT TRYING TO SEE WHAT THE PHYSICIAN IS DOING AT THE COMPUTER

And because there's no password to enter in the exam room, patients can't learn your password simply by watching you enter it.

15. SCREEN SHOT OF A PATIENT RECORD OR MEDICATION LIST

BARB also allows only authorized personnel to log onto CIS, giving our patients the assurance that their health information is private and secure.

15A. PHYSICIAN HITS F3 AND PROGRAM LOGS OFF

11. BARB 'ENROLLMENT' AREA - OUR PHYSICIAN ENTERS AREA, REMOVES HIS BARB AND PLACES IT BACK IN THE BOX. HE LEAVES THE AREA **SHOOT WITH ASSIGNED BARB TOO**

At the end of the day, simply return your BARB and it will deactivate.

FADE OUT

We've developed BARB to make your life easier – we hope it does.